Error Correction for Index Coding With Coded Side Information

Eimear Byrne, and Marco Calderini.

Abstract

Index coding is a source coding problem in which a broadcaster seeks to meet the different demands of several users, each of whom is assumed to have some prior information on the data held by the sender. A well-known application is to satellite communications, as described in one of the earliest papers on the subject [6]. It is readily seen that if the sender has knowledge of its clients' requests and their *side-information* sets, then the number of packet transmissions required to satisfy all users' demands can be greatly reduced if the data is encoded before sending. The collection of side-information indices as well as the indices of the requested data is described as an *instance $\mathcal{I}$* of the index coding with side-information (ICSI) problem. The encoding function is called the index code of $\mathcal{I}$, and the number of transmissions employed by the code is referred to as its *length*. The main ICSI problem is to determine the optimal length of an index code for and instance $\mathcal{I}$. As this number is hard to compute, bounds approximating it are sought, as are algorithms to compute efficient index codes. These questions have been addressed by several authors [1], [4], [5], [7], [33], [37], often taking a graph-theoretic approach. Two interesting generalizations of the problem that have appeared in the literature are the subject of this work. The first of these is the case of index coding with *coded side information* [10], [34], in which linear combinations of the source data are both requested by and held as users' side-information. This generalization has applications, for example, to relay channels and necessitates algebraic rather than combinatorial methods. The second is the introduction of error-correction in the problem, in which the broadcast channel is subject to noise [11]. In this paper we characterize the optimal length of a scalar or vector linear index code with coded side information (ICCSI) over a finite field in terms of a generalized *min-rank* and give bounds on this number based on constructions of random codes for an arbitrary instance. We furthermore consider the length of an optimal δ-error correcting code for an instance of the ICCSI problem and obtain bounds analogous to those described in [11], both for the Hamming metric and for rank-metric errors. We describe decoding algorithms for both categories of errors based on those given in [11], [35].

Index Terms

Index coding, min-rank, error correction, minimum distance, network coding, coded side information.

Error Correction for Index Coding With Coded Side Information

I. INTRODUCTION

The problem of index coding with side information (ICSI) was introduced by Birk and Kol in [6] under the term *informed source coding on demand*. In [4] the authors explicitly refer to the problem as *index coding*. This topic is motivated by applications in broadcast communications such as audio and video on-demand, content delivery, and wireless networking. It relates to a problem of source coding with *side information*, in which receivers have partial information about the data to be sent prior to its broadcast. The problem for the sender is to exploit knowledge of the users' side information to encode data optimally, that is to reduce the overall length of the encoding, or equivalently, the number of transmitted packets. The ICSI problem has since become a subject of several studies and generalizations [1], [4], [5], [31], [11], [12], [33].

The scenario of the ICSI problem is the following. A server (sender) has to broadcast some data to a set of clients (receivers or users), with possibly different messages requested by different clients. Before the transmission starts, each receiver already has some data in its possession, its cached packets, called its side-information. These packets may be from a previous broadcast, perhaps sent during lighter data traffic periods, or acquired by some other communication. The receivers let the sender know which messages they have, and which they require. The broadcaster can use this information, along with encoding, to reduce the overall number of packet transmissions required to satisfy all the demands of its clients. If the sender has been successful in this endeavour, then the broadcasted data can be utilized by each user, along with its cached packets, in order to decode its own specific demand.

The main index coding problem is to determine the minimum number of packet transmissions required by the sender in order to satisfy all users' requests, if encoding of data is permitted. Given an instance of the ICSI problem, Bar-Yossef *et al* [4] proved that finding the best *scalar linear* binary index code is equivalent to finding the *min-rank* of a graph, which is known to be an NP-hard problem [30]. The twin problem is to determine an explicit optimal encoding function for an instance. Any encoding function for an instance necessarily gives an upper bound on the optimal length of an index code. There have been a number of papers addressing this aspect of the problem, in fact finding sub-optimal but feasible solutions, using linear programming methods to obtain partitions of the users into solvable subsets. Such solutions involve obtaining *clique covers, partial-clique covers, multicast partitions* and some variants of these [7], [8], [33], [34], [37]. Other than these LP approaches, low-rank matrix completion methods may also be applied. This was considered for index coding over the real numbers in [22].

The importance of the index coding problem can also be seen in its equivalences and connections to other problems, such as *network coding*, *coded-caching* and *interference alignment* [15], [31], [16], [29]. These equivalences mean that results in index coding have impact in such other areas, and vice versa.

In [34], [10] the authors give a generalization of the index coding problem in which both demanded packets and locally cached packets may be linear combinations of some set of data packets. We refer to this as the *index coding with coded side information* problem (ICCSI). This represents a significant departure from the ICSI problem in that an ICCSI instance no longer has an obvious association to a graph, digraph or hypergraph, as in the ICSI case. However, as we show here, it turns out that many of the results for index coding have natural extensions in the ICCSI problem.

One motivation for the ICCSI generalization is related to the coded-caching problem. The method in [16] uses uncoded cache placement, but the authors give an example to show that coded cache placement performs better in general. In [17], it is shown that in a small cache size regime, when the number of users is not less than the number of files, a scheme based on coded cache placement is optimal. Moreover in [18] the authors show that the only way to improve the scheme given in [16] is by coded cache placement.

Another motivation is toward applications for wireless networks with relay helper nodes and cloud storage systems (see [10] and the references therein). Consider the example in Table I. We have a scenario with one sender and four receivers U_1, U_2, U_3 and U_4. The source node has four packets X_1, X_2, X_3 and X_4 and for $i = 1, ..., 4$ user U_i wants packet X_i. The transmitted packet is subject to independent erasures. It is assumed that there are feedback channels from the users, informing the transmitting node which packets are successfully received. At the beginning, in time slot 1, 2, 3 and 4 the source node transmits packets X_1, X_2, X_3 and X_4, respectively. After time slot 4 we have the following setting: U_1 has packet X_2, U_2 has packet X_1, U_3 has packet X_4 and U_4 has packet X_4. Now from the classical ICSI problem we have that receivers U_1 and U_2 form a clique, in the associated graph, and then we can satisfy their request sending $X_1 + X_2$. Similarly for U_3 and U_4 we can use $X_3 + X_4$. So, the source node in time slot 5 and 6 transmits the coded packet $X_1 + X_2$ and $X_3 + X_4$, intending that users receive the respective packet. However, U_1 and U_2 receive the coded packet $X_3 + X_4$ and U_3 and U_4 receive $X_1 + X_2$. At this point if only the uncoded packets in their caches are used, we still need to send two packets. If all packets in their caches are used, the source only needs to transmit one coded packet $X_1 + X_2 + X_3 + X_4$ in time slot 7. If all four users can receive this last transmission successfully, then all users can decode the required packets by linearly combining with the packets received earlier.

Time slot	Packet sent	Received by U_1?	Received by U_2?	Received by U_3?	Received by U_4?
1	X_1	no	yes	no	no
2	X_2	yes	no	no	no
3	X_3	no	no	no	yes
4	X_4	no	no	yes	no
5	$X_1 + X_2$	no	no	yes	yes
6	$X_4 + X_3$	yes	yes	no	no
7	$X_1 + X_2 + X_3 + X_4$	yes	yes	yes	yes

TABLE I
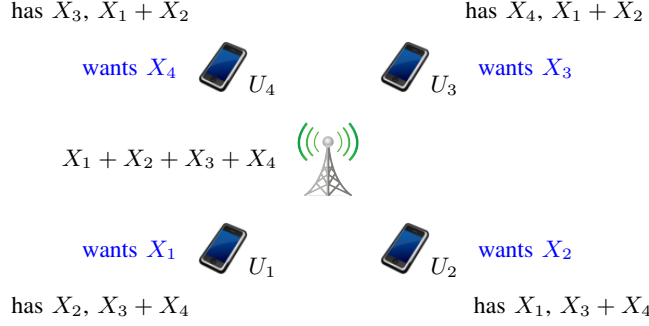ILLUSTRATION OF UTILIZING CODED PACKETS AS SIDE INFORMATION.

Fig. 1. State of network after time slot 6.

A second generalization of the ICSI problem was given in [11], where the authors consider error correction. That is, the broadcast channel may be subject to noise during a transmission. Classical coding theory plays a role in several of the results and a number of bounds are given on the optimal length of an *error correcting index code* (ECIC) that corrects some δ Hamming errors. A decoding algorithm based on syndrome decoding is also described. We remark that error-correction for network coding has only been addressed for multicast, where rank-metric and subspace codes are proposed. There are numerous papers on this subject after the seminal works [25], [36]. Many of these are based on Gabidulin codes [20].

A. Our Contribution

In this paper we develop the theory of index coding further along the lines of these latter mentioned generalizations. That is, we consider the ICCSI problem both in the error-free case and with respect to error correction. We assume that the source data is composed of n blocks of length t over $\mathbb{F}_q$ (the finite field of q elements), and that encoding involves taking $\mathbb{F}_q$-linear combinations of the n data blocks. In particular, we consider both linear and scalar-linear index codes. We describe a generalized min-rank for the ICCSI problem, which we show gives the optimal length for $\mathbb{F}_q$-linear encodings. This quantity is actually shown to be the minimum rank weight of the coset of an $\mathbb{F}_q$-linear matrix code determined by an ICCSI instance. We characterize necessary and sufficient conditions for a matrix L to *realize* an instance of the ICCSI problem and use this to obtain upper bounds on the length of an optimal $\mathbb{F}_q$-linear index code with coded side information. The first of these may be viewed as a generalization of the bound obtained by the existence of a partial clique in the *side-information graph* of a classical index coding problem. It requires q to be large although it does not rely on the use of a *maximum distance separable* (MDS) code. The second of these bounds offers a refinement and relaxation of the constraint on q and is not explicit. Both are based on the probability that an arbitrary matrix realizes a code for an instance.

Following the work of [11], we consider error correction for the ICCSI problem, both for the Hamming and rank metric and address the question of the main index coding problem for error correcting index codes. We establish criteria for error correction for an ICCSI instance and give bounds on the optimal length of a δ-error correcting ECIC, both for the Hamming metric and the rank metric. These results are extensions of the κ, α and sphere-packing and Singleton bounds as described in [11]. Some of these also yield further upper bounds on the optimal length of an ICCSI code for the error-free case.

Finally, we outline decoding strategies for linear ECICs for both the rank and Hamming distance. In the first case we extend the syndrome decoding method to correct Hamming errors for index codes given in [11] to the ICCSI case. In the second, we show that the simple, low-complexity strategy for additive matrix channels given in [35] can be applied to correct rank-metric errors, that is to handle error matrices of rank upper bounded by some δ.

II. PRELIMINARIES

We establish notation to be used throughout the paper. For any positive integer n, we let $[n] := \{1, \ldots, n\}$. We write $\mathbb{F}_q$ to denote the finite field of order q and use $\mathbb{F}_q^{n \times t}$ to denote the vector space of all $n \times t$ matrices over $\mathbb{F}_q$. Given a matrix $X \in \mathbb{F}_q^{n \times t}$ we write X_i and X^j to denote the ith row and jth column of X, respectively. More generally, for subsets $\mathcal{S} \subset [n]$

and $\mathcal{T} \subset [t]$ we write $X_{\mathcal{S}}$ and $X^{\mathcal{T}}$ to denote the $|\mathcal{S}| \times t$ and $n \times |\mathcal{T}|$ submatrices of X comprised of the rows of X indexed by $\mathcal{S}$ and the columns of X indexed by $\mathcal{T}$ respectively. We write $\langle X \rangle$ to denote the row space of X.

In this work we will consider two distance functions, namely the Hamming metric and the rank metric, over the $\mathbb{F}_q$-vector space $\mathbb{F}_q^{n \times t}$.

Choosing a basis of the finite field of q^t elements, it is easy to see that $\mathbb{F}_{q^t}$ and $\mathbb{F}_q^{n \times t}$ are isomorphic as $\mathbb{F}_q$-vector spaces. Then, given the usual definition of the Hamming distance between a pair of elements $x, y \in \mathbb{F}_{q^t}^n$:

$$d_H(x, y) := |\{i : x_i \neq y_i\}|,$$

we define the Hamming distance between a pair of matrices $X, Y \in \mathbb{F}_q^{n \times t}$ as the number of coordinates in $[n]$ such that $X_i \neq Y_i$, so the number of differing rows of X and Y.

For two matrices $A, B \in \mathbb{F}_q^{n \times t}$, the rank distance between A and B is the rank of the matrix $A - B$ over $\mathbb{F}_q$:

$$d_{\mathrm{rk}}(A, B) = \mathrm{rk}(A - B).$$

We write $d(A, B)$ to denote either distance function between A and B and we write $w(A)$ to denote $d(A, 0)$. Given A and a set $\mathcal{S}$, $d(A, \mathcal{S}) = \min\{d(A, S) : S \in \mathcal{S}\}$. In some cases we will specify explicitly which distance function should be understood, otherwise the reader should interpret d or w as denoting either metric.

Recall that for any pair of subspaces U and V, their sum is the subspace $U + V = \{u + v : u \in U, v \in V\}$ and we write $U \oplus V$ to denote the direct sum $U \oplus V = \{(u, v) : u \in U, v \in V\}$. Moreover $U + V$ and $U \oplus V$ are isomorphic if and only if $U \cap V$ is the trivial space. For arbitrary x in the ambient space, the coset $x + U := \{x + u : u \in U\}$. We use the standard notation $U < V$ to denote that U is a subspace of V.

III. INDEX CODING WITH CODED SIDE INFORMATION

In [34] the authors generalized the index coding problem so that coded packets of a data matrix X may be broadcast or part of a user's cache. As mentioned before, this finds applications, in broadcast channels with helper relay nodes.

Before we present the model with coded side information, let us recall the scenario for uncoded side information (see [11], [12]). In that case, the data is a vector $X \in \mathbb{F}_q^n$ possessed by a single sender. There are m users or receivers, each of which has an index set $\mathcal{X}_i \subset [n]$, called its side-information. This indicates that the ith user possesses the entries of X indexed by $\mathcal{X}_i$. The surjection $f : [m] \longrightarrow [n]$ assigns users to indices, indicating that User i wants $X_{f(i)}$ and it is also assumed that $f(i) \notin \mathcal{X}_i$. The sender is assumed to be informed of the values $f(i)$ and $\mathcal{X}_i$ of each user.

We now describe an instance of index coding with coded-side information. There is a data matrix $X \in \mathbb{F}_q^{n \times t}$ and a set of m receivers or users. X is thus a list of n blocks of length t over $\mathbb{F}_q$. For each $i \in [m]$, the ith user seeks some linear combination of the rows of X, say $R_i X$ for some $R_i \in \mathbb{F}_q^n$. We'll refer to R_i as the request vector and to $R_i X$ as the request packet of User i. A user's cache denotes locally stored data, which it can freely access. In our model it is represented by a pair of matrices

$$V^{(i)} \in \mathbb{F}_q^{d_i \times n} \text{ and } \Lambda^{(i)} \in \mathbb{F}_q^{d_i \times t}$$

related by the equation

$$\Lambda^{(i)} = V^{(i)} X.$$

While the matrix X may be unknown to User i, it is assumed that any vector in the row spaces of $V^{(i)}$ and $\Lambda^{(i)}$ can be generated at the ith receiver. We denote these respective row spaces by $\mathcal{X}^{(i)} := \langle V^{(i)} \rangle$ and $\mathcal{L}^{(i)} := \langle \Lambda^{(i)} \rangle$ for each i. The side information of the ith user is $(\mathcal{X}^{(i)}, \mathcal{L}^{(i)})$. Similarly, the sender S has the pair of row spaces $(\mathcal{X}^{(S)}, \mathcal{L}^{(S)})$ for matrices

$$V^{(S)} \in \mathbb{F}_q^{d_S \times n} \text{ and } \Lambda^{(S)} = V^{(S)} X \in \mathbb{F}_q^{d_S \times t}$$

and does not necessarily possess the matrix X itself.

The ith user requests a coded packet $R_i X \in \mathcal{L}^{(S)}$ with $R_i \in \mathcal{X}^{(S)} \backslash \mathcal{X}^{(i)}$. We denote by R the $m \times n$ matrix over $\mathbb{F}_q$ with each ith row equal to R_i. The matrix R thus represents the requests of all m users. We denote by

$$\mathcal{X} := \{A \in \mathbb{F}_q^{m \times n} : A_i \in \mathcal{X}^{(i)}, i \in [m]\},$$

so that $\mathcal{X} = \oplus_{i \in [m]} \mathcal{X}^{(i)}$ is the direct sum of the $\mathcal{X}^{(i)}$ as a vector space over $\mathbb{F}_q$.

We define $\tilde{\mathcal{X}} := \{Z \in \mathbb{F}_q^{m \times n} : Z_i \in \mathcal{X}^{(S)}\}$, which may be viewed as the direct sum of m copies of $\mathcal{X}^{(S)}$.

Remark III.1. *The reader will observe that the classical ICSI problem is indeed a special case of the index coding problem with coded side information (cf. [11], [12]). Setting $V^{(S)}$ to be the $n \times n$ identity matrix, $R_i = \mathbf{e}_{f(i)} \in \mathbb{F}_q^n$ and $V^{(i)}$ to be the $d_i \times n$ matrix with rows $V_j^{(i)} = \mathbf{e}_{i_j}$ for each $i_j \in \mathcal{X}_i$, yields $\mathcal{X}^{(i)} = \langle \mathbf{e}_j : j \in \mathcal{X}_i \rangle$. Then User i has the rows of X indexed by $\mathcal{X}_i$ and requests $X_{f(i)}$.*

Remark III.2. *The case where the sender does not necessarily possess the matrix X itself can be applied to the* broadcast relay channel, *as described in [34]. The authors consider a channel as in Fig. 2, and assume that the relay is close to the*
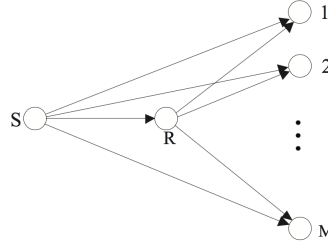
Fig. 2. Broadcast Relay Channel

users and far away from the source, and in particular that all relay-user links are erasure-free. Each node is assumed to have some storage capacity and stores previously received data in its cache. The packets in the cache of the relay node are obtained as previous broadcasts, hence it may contain both coded and uncoded packets. The relay node, playing the role of the sender, transmits packets obtained by linearly combining the packets in its cache, depending on the requests and coded side information of all users. It seeks to mimimize the total number of broadcasts such that all users' demands are met.

Definition III.3. An instance of the Index Coding with Coded Side Information (ICCSI) problem is a list $\mathcal{I} = (t, m, n, \mathcal{X}, \mathcal{X}^{(S)}, R)$ for some positive integers t, m, n, subspaces $\mathcal{X}^{(S)}$ and $\mathcal{X}^{(i)}$ of $\mathbb{F}_q^n$ of dimensions d_S, d_i for $i \in [m]$ such that $\mathcal{X} = \oplus_{i \in [m]} \mathcal{X}^{(i)}$ and a matrix R in $\tilde{\mathcal{X}}$.

For the remainder, we let $t, m, n, \mathcal{X}, \mathcal{X}^{(S)}, \tilde{\mathcal{X}}, R$ be as described above and we fix $\mathcal{I} = (t, m, n, \mathcal{X}, \mathcal{X}^{(S)}, R)$ to denote an instance of the ICCSI problem for these parameters. We now define what is meant by an index code for an instance $\mathcal{I}$: it is essentially a map that encodes any data matrix X in such a way that each user, given its side-information and received transmission, can uniquely determine its requested packet $R_i X \in \mathbb{F}_q^t$.

Definition III.4. Let N be a positive integer. We say that the map

$$E : \mathbb{F}_q^{n \times t} \to \mathbb{F}_q^{N \times t},$$

is an $\mathbb{F}_q$-code for $\mathcal{I}$ of length N if for each ith receiver, $i \in [m]$ there exists a decoding map

$$D_i : \mathbb{F}_q^{N \times t} \times \mathcal{X}^{(i)} \to \mathbb{F}_q^t,$$

satisfying

$$\forall X \in \mathbb{F}_q^{n \times t} \: : \: D_i(E(X), A) = R_i X,$$

for some vector $A \in \mathcal{X}^{(i)}$, in which case we say that E is an $\mathcal{I}$-IC. E is called an $\mathbb{F}_q$-linear $\mathcal{I}$-IC if $E(X) = LV^{(S)} X$ for some $L \in \mathbb{F}_q^{N \times d_S}$, in which case we say that L represents the code E, or that the matrix L realizes E. If $t = 1$, we say that L represents a scalar linear index code. If $t > 1$ we say that the code is vector linear. We write $\mathcal{L}$ to denote the space $\langle LV^{(S)} \rangle$.

An encoding is sought such that the length N of the $\mathcal{I}$-IC is as small as possible. We shall be principally concerned with $\mathbb{F}_q$-linear codes for an instance $\mathcal{I}$. We assume that the side information matrices $V^{(i)}$ of all users are known to the sender, along with the demand vectors R_i. As we'll see in the next section, this knowledge is sufficient to determine an encoding matrix L for an $\mathbb{F}_q$-linear $\mathcal{I}$-IC. These assumptions are in keeping with those outlined in [6] for the original *informed source coding on demand problem* and are based on the existence of a slow error-free reverse channel allowing communication from users to the sender. We also assume that $LV^{(S)}$ is known to the receivers before the broadcast of the encoded matrix $LV^{(S)} X$. This knowledge, along with the transmission $LV^{(S)} X$ and its own cache data will be used by each ith user in order to compute its demand $R_i X$. These assumptions mean that the gains of encoding an ICCSI instance are greater as t increases.

A. Necessary and Sufficient Conditions for Realization of an $\mathbb{F}_q$-Linear $\mathcal{I}$-IC

In the following we give necessary and sufficient conditions for a matrix L to represent a linear code of the instance $\mathcal{I}$ (in fact the sufficiency of the statement of Lemma III.5 has already been noted in [34]).

Lemma III.5. *Let $L \in \mathbb{F}_q^{N \times d_S}$. Then L represents an $\mathbb{F}_q$-linear $\mathcal{I}$-IC index code of length N if and only if for each $i \in [m]$, $R_i \in \mathcal{L} + \mathcal{X}^{(i)}$.*

Proof: Let $i \in [m]$ and let $R_i \in \mathcal{X}^{(S)}$. Suppose that $Y = LV^{(S)} X$ has been transmitted. If $R_i \in \mathcal{L} + \mathcal{X}^{(i)}$ then there exist $A \in \mathbb{F}_q^{d_i}, B \in \mathbb{F}_q^N$ such that $R_i = AV^{(i)} + BLV^{(S)}$. Then for any $X \in \mathbb{F}_q^{n \times t}$ we have

$$R_i X = AV^{(i)} X + BLV^{(S)} X = A\Lambda^{(i)} + BY.$$

Therefore, Receiver i, knowing $V^{(i)}X$ and $\Lambda^{(i)}$, can compute A and B and hence acquires R_iX.

Conversely, suppose that $R_i \notin \mathcal{L} + \mathcal{X}^{(i)}$. Then for each $U \in \mathbb{F}_q^t$, we have

$$
\mathrm{rank}\left(\begin{bmatrix} R_i & U \\ V^{(i)} & \Lambda^{(i)} \\ LV^{(S)} & Y \end{bmatrix}\right) = 1 + \mathrm{rank}\left(\begin{bmatrix} V^{(i)} & \Lambda^{(i)} \\ LV^{(S)} & Y \end{bmatrix}\right)
$$

$$
= 1 + \mathrm{rank}\left(\begin{bmatrix} V^{(i)} \\ LV^{(S)} \end{bmatrix}\right) = \mathrm{rank}\left(\begin{bmatrix} R_i \\ V^{(i)} \\ LV^{(S)} \end{bmatrix}\right).
$$

In particular, the linear system

$$
R_iX = U, V^{(i)}X = \Lambda^{(i)}, LV^{(S)}X = Y
$$

is consistent for each $U \in \mathbb{F}_q{}^t$. It follows that

$$
Pr(R_iX = U | V^{(i)}X = \Lambda^{(i)}, LV^{(S)}X = Y) = \frac{1}{q^t}, \tag{1}
$$

so the side information of R_i conveys no information about R_iX to the ith receiver. ∎

Lemma III.5 simply says that the demands of all users can be simultaneously satisfied if and only if for each i the smallest vector space containing both $\mathcal{L}$ and $\mathcal{X}^{(i)}$ also contains R_i; in other words extending the side-information spaces $\mathcal{X}^{(i)}$ by the same space $\mathcal{L}$ in each case contains the ith request vector. This is achieved, for example, if $\mathcal{L} + \mathcal{X}^{(i)}$ is the space $\mathcal{X}^{(S)}$ for each i, although this is clearly not necessary.

An equivalent formulation of the statement of Lemma III.5 is to say that L represents a linear index code for $\mathcal{I}$ if and only if $\mathcal{L}$ meets each coset $R_i + (\mathcal{X}^{(i)} \cap \mathcal{X}^{(S)}) = \{R_i + A : A \in \mathcal{X}^{(i)} \cap \mathcal{X}^{(S)}\}$. We will use this view to obtain an upper bound on the optimal length on a linear index code in Theorem III.18.

Given an $\ell \times n$ matrix $A \in \mathbb{F}_q^{\ell \times n}$, we write $A^\perp$ to denote the null space of A in $\mathbb{F}_q^n$. Furthermore, for each $i \in [m]$ we define the sets:

$$
\begin{aligned}
\mathcal{Y}^{(i)} &:= \{Z \in \mathbb{F}_q^{n \times t} : V^{(i)}Z = 0\} = (V^{(i)\perp})^t, \\
\mathcal{Z}^{(i)} &:= \{Z \in \mathbb{F}_q^{n \times t} : V^{(i)}Z = 0, R_iZ \neq 0\}.
\end{aligned}
$$

To help put these sets in context, if $V^{(i)}$ has rows composed of standard basis vectors, say with leading ones indexed by the set $\mathcal{S}^i \subset [n]$ (which means the side-information of User i is uncoded) then $\mathcal{Y}^{(i)}$ consists of those matrices whose columns indexed by $\mathcal{S}^i$ are all-zero. Then $\mathcal{Y}^{(i)}$ can be identified with the set $[n]\backslash\mathcal{X}_i$, the complement of the side information of user i and $\mathcal{Z}^{(i)}$ can be identified with $[n]\backslash\mathcal{X}_i \cup \{f(i)\}$.

Remark III.6. *In the classical ICSI problem, two data matrices X and X' are called* confusable *at receiver i (cf. [2]) if they yield the same side information for i, i.e. $X_j = X'_j$ for all $j \in \mathcal{X}_i$, and if moreover the packets $X_{f(i)}$ and $X'_{f(i)}$ are different (here $\mathcal{X}_i$ represents the side information of the receiver i and $f(i)$ the request packet). In the ICCSI problem, two vectors X, X' are called confusable at receiver i if $V^{(i)}X = V^{(i)}X'$ and $R_iX \neq R_iX'$, i.e. if they yield the same side information for the ith user but the requested data packets are different. Therefore, X and X' are confusable at receiver i if and only if $X - X'$ lies in the set $\mathcal{Z}^{(i)}$.*

The essential content of next result, which follows from Lemma III.5, is that L represents a linear code of $\mathcal{I}$ if and only if any confusable pair X, X' result in different encodings. Therefore, another way of stating Corollary III.7 is:

L represents an $\mathbb{F}_q$-linear $\mathcal{I}$-IC if and only if $LV^{(S)}X \neq LV^{(S)}X'$ for any confusable pair $X, X' \in \mathbb{F}_q^{n \times t}$.

Then L realizes and $\mathbb{F}_q$-linear $\mathcal{I}$-IC if and only if no matrix of $\mathcal{Z}^{(i)}$ vanishes after multiplication by $LV^{(S)}$, so $\mathcal{Z}^{(i)}$ may be used to characterize all linear codes of $\mathcal{I}$. Of course $LV^{(S)}Z$ is non-zero if and only if it has positive weight. This result will be generalized further in Theorem IV.2 to give a criterion for error-correction.

Corollary III.7. *Let $L \in \mathbb{F}_q^{N \times d_S}$. Then L represents an $\mathbb{F}_q$-linear $\mathcal{I}$-IC of length N if and only if $LV^{(S)}Z \neq 0$ for each $i \in [m]$, and $Z \in \mathcal{Z}^{(i)}$.*

Proof: Fix some $i \in [m]$ and let $Z_0 \in \mathcal{Z}^{(i)}$, let $LV^{(S)}Z_0 = W$. Suppose that $R_i \notin \mathcal{L} + \mathcal{X}^{(i)}$. Then as in the proof of Lemma III.5, the linear system

$$
R_iZ = U, V^{(i)}Z = 0, LV^{(S)}Z = W \tag{2}
$$

is consistent for every choice of $U \in \mathbb{F}_q^n$. In particular, (2) has a solution Z_1 for $U = 0$. Then $Z = Z_0 - Z_1 \in \mathcal{Z}^{(i)}$ and $LV^{(S)}Z = 0$. We have shown that if L does not represent a linear code for $\mathcal{I}$ then for some i, there exists $Z \in \mathcal{Z}^{(i)}$ such that

$LV^{(S)}Z = 0$. Applying the contrapositive, this yields that if $\mathrm{rank}(LV^{(S)}Z) \geq 1$ (i.e. if $LV^{(S)}Z \neq 0$) for each $i \in [m]$ and $Z \in \mathcal{Z}^{(i)}$, then L represents a linear index code for the instance $\mathcal{I}$.

Conversely, if there exist $A \in \mathbb{F}_q^{d_i}, B \in \mathbb{F}_q^N$ such that $R_i = AV^{(i)} + BLV^{(S)}$ then

$$R_i Z = AV^{(i)}Z + BLV^{(S)}Z = BLV^{(S)}Z \neq 0,$$

for any $Z \in \mathcal{Z}^{(i)}$. ∎

B. The Optimal Length of an $\mathbb{F}_q$-Linear $\mathcal{I}$-IC

We extend the definition of the min-rank of an instance of the ICSI problem, as given in [12], to the ICCSI problem. We will show that this characterizes the shortest possible length of an $\mathbb{F}_q$-linear $\mathcal{I}$-IC.

Definition III.8. We define the min-rank of the instance $\mathcal{I}$ of the ICCSI problem over $\mathbb{F}_q$ to be

$$\kappa(\mathcal{I}) \;=\; \min\{\mathrm{rank}(A + R) : A \in \mathbb{F}_q^{m \times n}, A_i \in \mathcal{X}^{(i)} \cap \mathcal{X}^{(S)} \subset \mathbb{F}_q^n, \; \forall i \in [m]\}.$$

Observe that the quantity $\kappa(\mathcal{I})$ is $d_{\mathrm{rk}}(R, \mathcal{X} \cap \tilde{\mathcal{X}})$, which is the rank-distance of $R \in \mathbb{F}_q^{m \times n}$ to the $\mathbb{F}_q$-linear code $\mathcal{X} \cap \tilde{\mathcal{X}}$, or equivalently the minimum rank-weight of the coset $R + (\mathcal{X} \cap \tilde{\mathcal{X}}) \subset \mathbb{F}_q^{m \times n}$.

We now show that given the instance $\mathcal{I}$, the minimum length of an $\mathbb{F}_q$-linear $\mathcal{I}$-IC is given by its min-rank.

Lemma III.9. *The length of an optimal $\mathbb{F}_q$-linear $\mathcal{I}$-IC is $\kappa(\mathcal{I})$.*

Proof: Let $L \in \mathbb{F}_q^{N \times d_S}$ have rank N. From Lemma III.5, L represents a linear code of length N if and only if for each $i \in [m]$ there exist $A_i \in \mathcal{X}^{(i)} \cap \mathcal{X}^{(S)} \subset \mathbb{F}_q^n, B_i \in \mathbb{F}_q^N$ such that

$$R_i = B_i L V^{(S)} - A_i,$$

(i.e. if and only if $R_i \in \mathcal{L} + \mathcal{X}^{(i)}$ for each i). Equivalently this holds if and only if there exist matrices $A \in \mathcal{X} \cap \tilde{\mathcal{X}}, B \in \mathbb{F}_q^{m \times N}$ such that $R = BLV^{(S)} - A$, in which case we have $BLV^{(S)} = R + A$ in the coset $R + (\mathcal{X} \cap \tilde{\mathcal{X}})$. In particular, we have shown that every matrix $L \in \mathbb{F}_q^{N \times d_S}$ represents an $\mathbb{F}_q$-linear code for $\mathcal{I}$ only if

$$BLV^{(S)} \in R + (\mathcal{X} \cap \tilde{\mathcal{X}})$$

for some $B \in \mathbb{F}_q^{m \times N}$, so every such L has rank at least $\kappa(\mathcal{I})$.

Now let $A \in \mathbb{F}_q^{m \times n}$ with $A_i \in \mathcal{X}^{(i)} \cap \mathcal{X}^{(S)}$ for each $i \in [m]$. Suppose that $A + R$ has rank N. Since $A, R \in \tilde{\mathcal{X}}$, there exists $Z \in \mathbb{F}_q^{m \times d_S}$ of rank N satisfying $A + R = ZV^{(S)}$. Furthermore, there exist $B \in \mathbb{F}_q^{m \times N}$ and $L \in \mathbb{F}_q^{N \times d_S}$ such that $Z = BL$. Then

$$R = A - BLV^{(S)}$$

so L represents a linear code of length N for the instance $\mathcal{I}$. The length N is minimized for $N = \kappa(\mathcal{I})$, so there exists some L of rank $\kappa(\mathcal{I})$ representing a linear code for $\mathcal{I}$. ∎

Lemma III.9 gives a naive algorithm for computation of a matrix L for an optimal linear $\mathcal{I}$-IC: put each element of $R + (\mathcal{X} \cap \tilde{\mathcal{X}})$ into row-echelon form and choose one of minimal rank $N = \kappa(\mathcal{I})$. The non-zero rows of this matrix yields the required $N \times d_S$ matrix L. We do not suggest this as a practical approach, since it requires $\mathcal{O}(d_S^3 q^\ell)$ operations, with $\ell = \dim \mathcal{X} \cap \tilde{\mathcal{X}}$. We mention this here to give a concrete illustration of the realization problem. As already observed in [11], the min-rank $\kappa(\mathcal{I})$ of the instance $\mathcal{I}$ generalizes the notion of the min-rank of the so-called side-information graph of the classical index coding problem, which is NP-hard to compute. A discussion on the various approaches to obtaining bounds on the optimal length of an index code can be read in [33], where the authors assert that graph-theoretic methods for constructing index coding schemes yield bounds on the optimal length of an index code, which are often out-performed by the min-rank. In fact all of these so called graph-theoretic methods, which use linear programming methods to obtain (possibly sub-optimal) solutions to the linear index coding problem can be extended to the ICCSI case. These results have been outlined in a separate forthcoming paper [8].

C. Upper Bounds on the Optimal Length of an $\mathbb{F}_q$-Linear $\mathcal{I}$-IC

We now give upper bounds on $\kappa(\mathcal{I})$, applying probabilistic arguments. The main results are Corollary III.13 and Theorem III.18, both of which show that with certain constraints on N, there exists an $\mathbb{F}_q$-linear $\mathcal{I}$-IC of length N. While both results essentially give lower bounds on the probability that a random $N \times d_S$ matrix L represents an $\mathbb{F}_q$-linear $\mathcal{I}$-IC, the key point is that these probabilities are positive, so that existence is guaranteed. It is from this observation that upper bounds on $\kappa(\mathcal{I})$ are achieved.

We will use the following theorem proved by Zippel [38] (see also [14], [32]). We state it here for finite fields.

Theorem III.10. *Let m, s be positive integers with $q > m$ and let $P(x_1, ..., x_s)$ be a non-zero multivariate polynomial in $\mathbb{F}_q[x_1, ..., x_s]$ for which the largest exponent of any variable x_i is at most m. If $(a_1, ...a_s)$ is chosen uniformly at random in $\mathbb{F}_q^s$ then the probability that $P(a_1, ..., a_s)$ equals zero is at most $1 - (1 - m/q)^s$.*

Remark III.11. *Before proving the following theorem, we note that if $X_1, \ldots, X_n$ are independent uniformly distributed random variables that take their values over a field $\mathbb{F}_q$, then the random variable*

$$Z_\ell = \sum_{i=1}^{\ell} \alpha_i X_i,$$

for some $\ell \in [n]$, $\alpha_i \in \mathbb{F}_q^\times = \mathbb{F}_q \backslash \{0\}$, has a uniform distribution.

This is easily shown by an inductive argument. Clearly $P(Z_1 = \beta) = \frac{1}{q}$ for any $\beta \in \mathbb{F}_q$ since $\alpha_1 \neq 0$. Moreover, for any $\ell \in [n], \beta \in \mathbb{F}_q$,

$$\begin{aligned} P(Z_\ell = \beta) &= P(Z_{\ell-1} = \beta - \alpha_\ell X_\ell) \\ &= \sum_{\gamma \in \mathbb{F}_q} P(X_\ell = \gamma) P(Z_{\ell-1} = \beta - \alpha_\ell \gamma) = \frac{1}{q}. \end{aligned}$$

Let m' be the number of distinct equivalence classes of $[m]$ under the relation $i \equiv j$ if $\mathcal{X}^{(i)} = \mathcal{X}^{(j)}$. Let $\tilde{m}$ be a set of m' representatives for the distinct equivalence classes of $[m]$.

Theorem III.12. *Let $\mathcal{I}$ be an instance of an ICCSI problem and let $N = \max\{n - d_i : i \in [m]\}$. Suppose that $q > m'$. If the entries of a matrix $L \in \mathbb{F}_q^{N \times d_S}$ are chosen uniformly at random in $\mathbb{F}_q$, then the probability that L represents a linear code for $\mathcal{I}$ is at least $(1 - m'/q)^{N d_S}$.*

Proof: From Corollary III.7, if $w\left(LV^{(S)}Z\right) \geq 1$ for each $Z \in \mathcal{Y}^{(i)}$ then L represents a code for $\mathcal{I}$. For each $i \in \tilde{m}$, let $Z^{(i)} \in \mathbb{F}_q^{n \times k_i}$ satisfy $V^{(i)} Z^{(i)} = 0$ and have rank $k_i = n - d_i$. Write $L^{(i)} = LV^{(S)} Z^{(i)}$. The matrix L represents a code for $\mathcal{I}$ if $L^{(i)}$ is a full-rank matrix for each $i \in \tilde{m}$, which holds if and only if there exists a non-zero $k_i \times k_i$ minor $M^{(i)}$ of $L^{(i)}$. Since the entries of L are uniformly distributed, so are the entries of $L^{(i)}$, from Remark III.11. Each such minor has the form $M^{(i)} = \sum_{\sigma \in S_{k_i}} sgn(\sigma) \prod_{j=1}^{k_i} L_{v_j}^{(i)\sigma(v_j)}$. Now $\prod_{i \in \tilde{m}} M^{(i)}$ may be viewed as a polynomial in $N d_S$ variables of degree $\sum_{i \in \tilde{m}} k_i \leq m'N$ with each variable appearing with multiplicity at most m' in any term. Then the probability that L represents a code for $\mathcal{I}$ is the probability that $\prod_{i \in \tilde{m}} M^{(i)}$ is non-zero, which from Lemma III.10 is at least $(1 - m'/q)^{N d_S}$, for $q > m'$. $\blacksquare$

Corollary III.13. *If $q > m'$ then $\kappa(\mathcal{I}) \leq \max\{n - d_i : i \in [m]\}$.*

Proof: Theorem III.12 guarantees the existence of some matrix $L \in \mathbb{F}_q^{N \times d_S}$ that represents an $\mathbb{F}_q$-linear $\mathcal{I}$-IC of length $N = \max\{n - d_i : i \in [m]\}$. The result is now immediate since $N \geq \kappa(\mathcal{I})$. $\blacksquare$

Remark III.14. *In fact Schwartz's result [32] gives the lower bound of $1 - \frac{m'(n-d)}{q}$ on the probability of an $N \times d_S$ matrix L representing an $\mathcal{I}$-IC, where d is the average of the $\{d_i : i \in [m]\}$. While this may give a higher lower bound, it places the restriction $m'(n - d) < q$ and so in particular yields a weaker version of Corollary III.13.*

Remark III.15. *Note that if for some i, $LV^{(S)}Z$ is non-zero for any $Z \in \mathcal{Y}^{(i)}$, then it satisfies the decoding criterion for any possible request vector $R_i \in \mathcal{X}^{(S)}$, and hence delivers all possible requests to User i. Therefore, Theorem III.12 and Corollary III.13 should be viewed in the context of similar results in [6], [37], which lead to* partial clique-cover *and* partition multicast *schemes. There is also a close association with the so-called* Main Network Coding Theorem *[19, Theorem 2.2] for multicast network coding. All of these results rely on the field size q being sufficiently large to invoke Zippel's theorem and its variants.*

Remark III.16. *The approach in [6] to construct a linear IC for a partial clique is based on* maximum distance separable (MDS) codes *(this can be used also in the more general case of a multicast group, as described in [37]). Any generator matrix of an MDS linear code of length n and dimension k is such that any k columns are linear independent. Suppose that $\mathcal{I}$ is an ICSI instance and that d_i is the number of uncoded packets X_j known to the receiver i. Let G be a generator matrix of an MDS code of length n and dimension $N = \max\{n - d_i : i \in [m]\}$. Then the sender can broadcast the following linear combination of the columns of G:*

$$X_1 G^1 + \ldots + X_n G^n.$$

Without loss of generality, suppose that some receiver i has $X_{N+1}, \ldots, X_n$, and can thus recover

$$X_1 G^1 + \ldots + X_N G^N.$$

From the MDS property of G, the first N columns of G form an invertible matrix so that the user can determine $(X_1, \ldots, X_N)$. In terms of Lemma III.5, the side-information is encoded by a matrix $V^{(i)} = [0|I]$ whose rows are standard basis vectors. Appending the N rows of G then results in a matrix with row space $\mathbb{F}_q^n$. In the above we get a matrix

$$\begin{bmatrix} G^{[N]} & G^{[n]\backslash[N]} \\ 0 & I \end{bmatrix},$$

which has rank n, so any possible request vector is contained in $\langle G \rangle + \mathcal{X}^{(i)}$.

However, this approach with MDS codes is not possible in the more general case of coded side information. Indeed, suppose we have $n = m = 4$, $\mathcal{X}^{(S)} = \mathbb{F}_2^4$, the user side-information determined by

$$V^{(1)} = \begin{bmatrix} 1 & 0 & 0 & 1 \end{bmatrix}, V^{(2)} = \begin{bmatrix} 0 & 0 & 0 & 1 \end{bmatrix}, V^{(3)} = \begin{bmatrix} 0 & 1 & 0 & 0 \end{bmatrix}, V^{(4)} = \begin{bmatrix} 0 & 0 & 1 & 0 \end{bmatrix},$$

and requests

$$R_1 = [1110], R_2 = [0100], R_3 = [0010], R_4 = [0001].$$

If the approach using an MDS code could be applied, then the matrix

$$G = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

defined over $\mathbb{F}_2$, could be used to encode a vector $X = [X_1, ..., X_4]^T$. It is easy to check that $R_1 \notin \langle G \rangle + \mathcal{X}^{(1)}$ and so from Lemma III.5 we have that Receiver 1 cannot decode. On other hand consider the matrix

$$L = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{bmatrix},$$

defined over $\mathbb{F}_2$. Following the proof of Theorem III.12 we have the matrices

$$Z^{(1)} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{bmatrix}, Z^{(2)} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{bmatrix}, Z^{(3)} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}, Z^{(4)} = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

It is easy to check that for each i $LZ^{(i)}$ is a 3×3 matrix of full rank. Then the matrix L represents a linear index code for our instance but L does not generate an MDS code. In fact, direct inspection shows that $\mathcal{L} + \mathcal{X}^{(i)} = \mathbb{F}_2^4$ for each i so that L realizes an $\mathbb{F}_2$-linear $\mathcal{I}$-IC for any choice of R. This is equivalent to multicast network coding.

We can remove the explicit constraint that $q > m'$ to obtain an alternative lower bound on the probability of a realizable linear solution to the ICCSI problem. A straightforward counting argument yields the following 'folklore' result, a proof of which we include for completeness. Recall that for positive integers $s \geq r$ the Gaussian coefficient

$$\begin{bmatrix} s \\ r \end{bmatrix}_q := \frac{\prod_{j=0}^{r-1}(q^s - q^j)}{\prod_{j=0}^{r-1}(q^r - q^j)}$$

denotes the number of r-dimensional subspaces contained in an s-dimensional space over $\mathbb{F}_q$. If $s < r$ this number is zero.

Lemma III.17. *Let W, V, S be subspaces of $\mathbb{F}_q^n$ with $W < V \cap S$ and of dimensions w, v and s respectively. Suppose that $S \cap V$ has dimension ℓ. The number of N-dimensional subspaces U of S satisfying $V \cap U \subset W$ is*

$$\sum_{r=0}^{w} q^{(\ell-r)(N-r)} \begin{bmatrix} w \\ r \end{bmatrix}_q \begin{bmatrix} s - \ell \\ N - r \end{bmatrix}_q.$$

Proof: Let M be an r-dimensional subspace of $V \cap S$. A basis $\{m_1, ..., m_r\}$ of M can be completed to a linearly independent N-set by appending some $m_{r+1}, ..., m_N \subset S \backslash V$ in

$$\prod_{j=\ell}^{\ell+N-r-1} (q^s - q^j) = q^{\ell(N-r)} \prod_{j=0}^{N-r-1} (q^{s-\ell} - q^j)$$

ways. There are $(q^N - q^r) \cdots (q^N - q^{N-1})$ choices of $m_{r+1}, ..., m_N$ in $M + \langle m_{r+1}, ..., m_N \rangle \backslash M$. Therefore there are $q^{(\ell-r)(N-r)} \begin{bmatrix} s - \ell \\ N - r \end{bmatrix}_q$ N-dimensional subspaces of S that meet V in a given r-dimensional subspace of V. The result now follows since there are $\begin{bmatrix} w \\ r \end{bmatrix}_q$ r-dimensional subspaces of W. ∎

We'll now apply Lemma III.17 for the case $W = \mathcal{X}^{(i)}$, $V = \langle R_i, \mathcal{X}^{(i)} \rangle$ to count the number of subspaces $\mathcal{L} \in \mathcal{X}^{(S)}$ contained in their intersection. This will tell us the number of subspaces $\mathcal{L}$ such that $R_i \notin \mathcal{L} + \mathcal{X}^{(i)}$.

Theorem III.18. *Let $\mathcal{I}$ be an instance of an ICCSI problem. For each $i \in [m]$, let $\dim(\mathcal{X}^{(i)} \cap \mathcal{X}^{(S)}) = w_i$. The probability that there exists an N-dimensional subspace $\mathcal{L}$ of $\mathcal{X}^{(S)}$ such that for each $i \in [m]$, $R_i \in \mathcal{L} + \mathcal{X}^{(i)}$, is at least*

$$1 - \begin{bmatrix} d_S \\ N \end{bmatrix}_q^{-1} \sum_{i=1}^{m} \sum_{r=0}^{w_i} q^{(w_i+1-r)(N-r)} \begin{bmatrix} w_i \\ r \end{bmatrix}_q \begin{bmatrix} d_S - w_i - 1 \\ N - r \end{bmatrix}_q.$$

In particular, there exists a linear $\mathcal{I}$-IC of length N if

$$\sum_{i=1}^{m} \sum_{r=0}^{w_i} q^{(w_i+1-r)(N-r)} \begin{bmatrix} w_i \\ r \end{bmatrix}_q \begin{bmatrix} d_S - w_i - 1 \\ N - r \end{bmatrix}_q < \begin{bmatrix} d_S \\ N \end{bmatrix}_q.$$

Proof: Let $i \in [m]$. An N-dimensional subspace $\mathcal{L}$ of $\mathcal{X}^{(S)}$ satisfies $R_i \in \mathcal{L} + \mathcal{X}^{(i)}$ if and only if $(R_i + \mathcal{X}^{(i)}) \cap \mathcal{L}$ is non-empty. The number of N-dimensional subspaces of $\mathcal{X}^{(S)}$, that miss $R_i + \mathcal{X}^{(i)}$ is the number of $\mathcal{L}$ that meet $\langle R_i, \mathcal{X}^{(i)} \rangle$ in a subspace of $\mathcal{X}^{(i)}$. Since $R_i \in \mathcal{X}^{(S)} \backslash \mathcal{X}^{(i)}$ by assumption, $\langle R_i, \mathcal{X}^{(i)} \rangle \cap \mathcal{X}^{(S)}$ has dimension $w_i + 1$. Then from Lemma III.17, the number of N-dimensional subspaces $\mathcal{L}$ in $\mathcal{X}^{(S)}$ that miss $R_i + \mathcal{X}^{(i)}$ (i.e. the number satisfying $R_i \notin \mathcal{L} + \mathcal{X}^{(i)}$), is

$$\sum_{r=0}^{w_i} q^{(w_i+1-r)(N-r)} \begin{bmatrix} w_i \\ r \end{bmatrix}_q \begin{bmatrix} d_S - w_i - 1 \\ N - r \end{bmatrix}_q.$$

The probability that an arbitrary N-dimensional subspace of $\mathcal{X}^{(S)}$ misses $R_i + \mathcal{X}^{(i)}$ is this number divided by $\begin{bmatrix} d_S \\ N \end{bmatrix}_q$. From the union bound, the probability that an arbitrary N-dimensional subspace of $\mathcal{X}^{(S)}$ misses every $R_i + \mathcal{X}^{(i)}$ is upper bounded by

$$\begin{bmatrix} d_S \\ N \end{bmatrix}_q^{-1} \sum_{i=1}^{m} \sum_{r=0}^{w_i} q^{(w_i+1-r)(N-r)} \begin{bmatrix} w_i \\ r \end{bmatrix}_q \begin{bmatrix} d_S - w_i - 1 \\ N - r \end{bmatrix}_q.$$

∎

Remark III.19. *In the above argument, by invoking the union bound, we have assumed the most extreme case. For each i, let $S^{(i)}$ denote the set of N-dimensional subspaces $\mathcal{L}$ of $\mathcal{X}^{(S)}$ such that*

$$\mathcal{X}^{(i)} \cap \mathcal{L} = \langle R_i, \mathcal{X}^{(i)} \rangle \cap \mathcal{L}.$$

Then the probability of a decoding failure is maximized when the size of the union of the $S^{(i)}$ is maximized. If the $S^{(i)}$ are pairwise disjoint we have

$$\left| \cup_{i \in [m]} S^{(i)} \right| = \sum_{i \in [m]} |S^{(i)}|,$$

and so the given bound is sharp. This occurs if no N-dimensional subspace is contained in the intersection of any pair of the $S^{(i)}$. Moreover, there is no length N $\mathbb{F}_q$-linear $\mathcal{I}$-IC if and only if $\cup_{i \in [m]} S^{(i)}$ contains all N-dimensional subspaces of $\mathcal{X}^{(S)}$.

Remark III.20. *Given an N-dimensional subspace $\mathcal{L} < \mathcal{X}^{(S)}$ Theorem III.18 often yields a better lower bound on the probability that $L \in \mathbb{F}_q^{N \times d_S}$ satisfying $\mathcal{L} = \langle LV^{(S)} \rangle$ represents a linear $\mathcal{I}$-IC. Furthermore, it establishes existence for the case $m \geq q$.*

Example III.21. Let $m = 6, n = 4, q = 2$ and let $\mathcal{X}^{(S)} = \mathbb{F}_q^4$. Suppose that $\mathcal{X}^{(i)}$ has dimension $d_i = 2$ for each $i \in \{1, ..., 6\}$. According to Theorem III.18, the probability of the existence of a 3×4 matrix L over $\mathbb{F}_2$ that represents a linear $\mathcal{I}$-IC with these parameters is at least 0.2, but is inconclusive for the existence of a 2×4 encoding matrix L. Indeed there are such $\mathcal{I}$-IC satisfying $\kappa(\mathcal{I}) = 3 > 2 = \max\{n - d_i : i \in [6]\}$, for example, $\mathcal{I}$ with user side-information determined by

$$V^{(1)} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, V^{(2)} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, V^{(3)} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix},$$

$$V^{(4)} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, V^{(5)} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix}, V^{(6)} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

and requests

$$R_1 = [1000], R_2 = [0100], R_3 = [0010], R_4 = [0001], R_5 = [0100], R_6 = [1000]$$

has min-rank equal to 3.

On the other hand, there are several examples of $\mathcal{I}$ for the same parameters that have min-rank equal to 2, such as that defined by:

$$V^{(1)} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, V^{(2)} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}, V^{(3)} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix},$$

q	N	d	m	Theorem III.12	Theorem III.18
4	1	9	2	0.001	0.500
4	1	9	3	9.536×10^{-7}	0.250
4	1	9	4	−	2.861×10^{-6}
4	2	8	2	9.536×10^{-7}	0.523
4	2	8	3	9.094×10^{-13}	0.285
4	2	8	4	−	0.046
4	3	7	2	9.313×10^{-10}	0.528
4	3	7	3	8.673×10^{-19}	0.293
4	3	7	4	−	0.057
4	3	6	2	9.094×10^{-13}	0.530
4	4	6	3	8.271×10^{-25}	0.295
4	4	6	4	−	0.060
4	5	5	2	8.881×10^{-16}	0.532
4	5	5	3	7.888×10^{-31}	0.296
4	5	5	4	−	0.061
4	6	4	2	8.673×10^{-19}	0.532
4	6	4	3	7.523×10^{-37}	0.298
4	6	4	4	−	0.064
4	7	3	2	8.470×10^{-22}	0.536
4	7	3	3	7.174×10^{-43}	0.304
4	7	3	4	−	0.072
4	8	2	2	8.271×10^{-25}	0.553
4	8	2	3	6.842×10^{-49}	0.329
4	8	2	4	−	0.106
4	9	1	2	8.077×10^{-28}	0.624
4	9	1	3	6.525×10^{-55}	0.437
4	9	1	4	−	0.249
4	9	1	5	−	0.062

TABLE II

q	N	d	m	Theorem III.18
4	2	9	16	1.4305×10^{-5}
4	3	8	16	0.0117
4	4	7	16	0.0148
4	5	6	16	0.0162
4	6	5	16	0.0191
4	7	4	16	0.0299
4	8	3	17	0.0155
4	9	2	21	0.0156
8	2	9	64	5.8673×10^{-8}
8	3	8	64	0.0017
8	4	7	64	0.0019
8	5	6	64	0.0019
8	6	5	64	0.0021
8	7	4	64	0.0038
8	8	3	65	0.0019
8	9	2	73	0.0019
16	2	9	256	2.3192×10^{-10}
16	3	8	256	0.0002
16	4	7	256	0.0002
16	5	6	256	0.0002
16	6	5	256	0.0002
16	7	4	256	0.0004
16	8	3	257	0.0002
16	9	2	273	0.0002

TABLE III

$$V^{(4)} = \begin{bmatrix} 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}, V^{(5)} = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, V^{(6)} = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix},$$

and requests

$$R_1 = [1100], R_2 = [0111], R_3 = [1010], R_4 = [1001], R_5 = [0100], R_6 = [1111].$$

We tabulate (see Table II) evaluations of the lower bound on the probability of the existence of linear $\mathcal{I}$-ICs with $\mathcal{X}^{(S)} = \mathbb{F}_4^{10}$ and length $N = 10 - d$ where $d_i = d$ for each ith user in $[m], m = m' > 1$. In each case, we find that the maximal value of $m' = m$ for which the bound of Theorem III.18 can be applied is $m = q$. However, existence for $m > q$ can be established by Theorem III.18 for $N > n - d$. In Table III we record parameters N and $d = 10 - N + 1$ of $\mathcal{I}$-IC known to exist using the bound of Theorem III.18 for a maximal number of users m.

IV. ERROR CORRECTION IN THE ICCSI PROBLEM

We now discuss error-correction in the ICCSI problem, extending the ideas presented in [11], in two ways. The first direction is in the context of coded-side information, as presented in [34], [10]. The second allows for error correction for the rank metric, in the transmission of matrices in $\mathbb{F}_q^{N \times t}$ when $t > 1$. For the remainder, we let $\mathcal{M} \subset \mathbb{F}_q^{n \times t}$ denote the message space associated with the ICCSI problem.

A. The ECIC Problem

Definition IV.1. Let $\mathcal{I}$ be an instance of an ICCSI problem and let N be a positive integer. We say that the map

$$E : \mathbb{F}_q^{n \times t} \to \mathbb{F}_q^{N \times t},$$

is a δ-error correcting code for $\mathcal{I}$ of length N, and say that E is an $(\mathcal{I}, \delta)$-ECIC, if for each ith receiver there exists a decoding map

$$D_i : \mathbb{F}_q^{N \times t} \times \mathcal{X}^{(i)} \to \mathbb{F}_q^t,$$

satisfying

$$D_i(E(X) + W, A) = R_i X$$

for all $X \in \mathcal{M}$ and $W \in \mathbb{F}_q^{N \times t}$, $w(W) \leq \delta$ for some vector $A \in \mathcal{X}^{(i)}$. E is called a linear code for $\mathcal{I}$, or an $\mathbb{F}_q$-linear $\mathcal{I}$-ECIC if $E(X) = LV^{(S)} X$ for some $L \in \mathbb{F}_q^{N \times d_S}$, in which case we say that L represents the linear $(\mathcal{I}, \delta)$-ECIC E.

The standard coding theory argument gives a criterion for the existence of a $(\mathcal{I}, \delta)$-ECIC, extending [11, Lemma 3.8]. The following result is the error correction analogue of Lemma III.5. It basically says that the ith receiver can correct up to δ errors and uniquely decode its requested packet $R_i X$ if any pair of confusable data matrices have encodings $LV^{(S)} X$ and $LV^{(S)} X'$ that are at distance at least $2\delta + 1$ apart.

Theorem IV.2. Let $\mathcal{I}$ be an instance of an ICCSI problem and let N be a positive integer. A matrix $L \in \mathbb{F}_q^{N \times d_S}$ represents a linear $(\mathcal{I}, \delta)$-ECIC if and only if for all $i \in [m]$ it holds that

$$w\left(LV^{(S)}(X - X')\right) \geq 2\delta + 1,$$

for all $X, X' \in \mathcal{M}$ such that $X - X' \in \mathcal{Z}^{(i)}$.

Proof: Let $L \in \mathbb{F}_q^{N \times d_S}$ represent a linear $\mathcal{I}$-IC. For each $X \in \mathbb{F}_q^{n \times t}$, define

$$B(X, \delta) = \{Y : Y = LV^{(S)} X + W, W \in \mathbb{F}_q^{N \times t}, w(W) \leq \delta\}.$$

It is not hard to see by an adaptation of the usual coding theory arguments that the ith receiver can correct δ errors if and only if

$$B(X, \delta) \cap B(X', \delta) = \emptyset$$

for each $X, X' \in \mathcal{M}$ such that $V^{(i)} X = V^{(i)} X'$ and $R_i X \neq R_i X'$.

For the Hamming metric, the argument is almost identical to that for a classical error-correcting code. Suppose then that $t > 1$ and that w measures the rank weight.
Let $X, X' \in \mathcal{M}$ such that $X - X' \in \mathcal{Z}^{(i)}$. Let $LV^{(i)} X = Z$ and let $LV^{(i)} X' = Z'$. Let $A = Z - Z'$ and suppose $w(A) = d \leq 2\delta$. We may assume that A is in row-echelon form. Thus we can write $A = W + W'$ with $w(W) = \delta$ and $w(W') = d - \delta \leq \delta$, where the first δ rows of W are the corresponding rows of A and the others are zero, and the rows indexed by $[d] \setminus [\delta]$ in W' are the corresponding rows of A and the remaining $N - d + \delta$ rows are zero. That is

$$A = \begin{bmatrix} A_{[\delta]} \\ A_{[d] \setminus [\delta]} \\ 0 \end{bmatrix}, \ W = \begin{bmatrix} A_{[\delta]} \\ 0 \\ 0 \end{bmatrix} \text{ and } W' = \begin{bmatrix} 0 \\ A_{[d] \setminus [\delta]} \\ 0 \end{bmatrix}.$$

Then $Z - W = Z' + W' \in B(X, \delta) \cap B(X', \delta)$, so if the requires spheres $B(X, \delta)$ are disjoint, L represents a linear $\mathcal{I}$-ECIC. Conversely, if $B(X, \delta) \cap B(X', \delta) \neq \emptyset$ then $Z + W = Z' + W'$ for some W and W', each having rank at most δ. Thus $Z - Z' = W' - W$ and in particular, by the triangular inequality, $w(Z - Z') \leq w(W') + w(W) \leq 2\delta$. ∎

Let $\mathcal{I}$ be an instance of the ICCSI problem and let $i \in [m]$. Let $X, X' \in \mathcal{M}$ such that $X - X' \in \mathcal{Z}^{(i)}$. For the case $t > 1$, for any $L \in \mathbb{F}_q^{N \times d_S}$ we have

$$w(LV^{(S)}(X - X')) = \text{rank}(LV^{(S)}(X - X')) \leq \text{rank}(V^{(S)}(X - X')) \leq w(X - X').$$

Then L does not represent a linear $(\mathcal{I}, \delta)$-ECIC if $\text{rank}(X - X') \leq 2\delta$. We therefore assume, for $t > 1$, that $\mathcal{M}$ is a subset of $\mathbb{F}_q^{n \times t}$ of minimum rank distance at least $2\delta + 1$, and furthermore that $\{V^{(S)} X : X \in \mathcal{M}\} \subset \mathbb{F}_q^{d_S \times t}$ has minimum rank

distance $2\delta + 1$. Delsarte's result [13, Theorem 5.4] yields that $|\mathcal{M}| \leq q^{(d_S - 2\delta)t}$. We define $\mathcal{M}^{\triangle} := \{X - X' : X, X' \in \mathcal{M}\}$. For the Hamming metric case, we assume $\mathcal{M} = \mathbb{F}_q^{n \times t}$.

We define the following sets for any non-negative integer δ:

$$
\begin{aligned}
\mathcal{Y}_\delta^{(i)} &:= \{A \in \mathcal{Y}^{(i)} : \operatorname{rank}(A) \geq 2\delta + 1\} \\
\mathcal{Z}_\delta^{(i)} &:= \{A \in \mathcal{Z}^{(i)} : \operatorname{rank}(A) \geq 2\delta + 1\}
\end{aligned}
$$

Clearly a matrix $L \in \mathbb{F}_q^{N \times d_S}$ represents a linear $(\mathcal{I}, \delta)$-ECIC if and only if for all $i \in [m]$ it holds that

$$
w\left(LV^{(S)}Z\right) \geq 2\delta + 1,
$$

for all $Z \in \mathcal{Z}^{(i)}$ if w is the Hamming metric and for all $Z \in \mathcal{Z}_\delta^{(i)} \cap \mathcal{M}^{\triangle}$ if w represents the rank metric.

Remark IV.3. *Note that if $\operatorname{rank}(LV^{(S)}Z) \geq 2\delta + 1$ whenever $Z \in \mathcal{Z}^{(i)}$ has rank at least $2\delta + 1$, then $\operatorname{rank}(LV^{(S)}Z) \geq r$ whenever $Z \in \mathcal{Z}^{(i)}$ has rank at least r for $r \in [2\delta + 1]$. This can be seen by the following inductive argument. Suppose $\operatorname{rank}(LV^{(S)}Z) \geq r$ whenever $\operatorname{rank}(Z) \geq r$ for some positive integer r and suppose there exists some such $Z \in \mathcal{Z}^{(i)}$. Let $X \in \mathcal{Z}^{(i)}$ have rank $r - 1$ and let $\mathcal{S}$ be set of $r - 1$ linearly independent columns of X. If $\operatorname{rank}(LV^{(S)}X) < r - 1$ then S cannot be completed to a linearly independent set of size r in $\mathcal{Z}^{(i)}$ by hypothesis, Then every column of Z is contained in the span of $\mathcal{S}$, so in particular the column space of X contains an r-dimensional space, which is impossible.*

B. Bounds on the Optimal Length of an Error Correcting Index Code

We denote by $\mathcal{N}(\mathcal{I}, \delta)$ the optimal length N of an $\mathbb{F}_q$-linear $(\mathcal{I}, \delta)$-ECIC. Clearly $\mathcal{N}(\mathcal{I}, 0) = \kappa(\mathcal{I})$. This section is devoted to obtaining bounds on this number. In [11] a number of bounds are discussed, namely the α-bound, κ-bound and Singleton bound. All of these bounds have extensions for Hamming metric $(\mathcal{I}, \delta)$-ECICs. The α-bound holds for rank metric $(\mathcal{I}, \delta)$-ECICs, but the question of the rank distance analogue of the κ-bound still open. We consider these two cases separately.

1) Hamming metric $(\mathcal{I}, \delta)$-ECICs: We assume throughout this section that w represents the Hamming weight and that $\mathcal{N}(\mathcal{I}, \delta)$ is the optimal length of an $\mathbb{F}_q$-linear Hamming metric $(\mathcal{I}, \delta)$-ECIC. We denote by $N(k, d)$ the optimal length ℓ of an $\mathbb{F}_q$-$[\ell, k, d]$ code, i.e. a k-dimensional $\mathbb{F}_q$-linear code in $\mathbb{F}_q^\ell$ of minimum Hamming distance d.

Thanks to the following result we can restrict our study to the case $t = 1$.

Lemma IV.4. *Let $t \geq 1$. Consider two instances $\mathcal{I} = (t, m, n, \mathcal{X}, \mathcal{X}^{(S)}, R)$ and $\mathcal{I}' = (1, m, n, \mathcal{X}, \mathcal{X}^{(S)}, R)$. Then a matrix $L \in \mathbb{F}_q^{N \times d_S}$ represents a linear $(\mathcal{I}, \delta)$-ECIC if and only if L represents a linear $(\mathcal{I}', \delta)$-ECIC.*

Proof: The matrices $V^{(i)}$, $V^{(S)}$ and the request vectors R_i's are the same for the two instances $\mathcal{I}$ and $\mathcal{I}'$. Let

$$
\mathcal{Z}_t^{(i)} = \{Z \in \mathbb{F}_q^{n \times t} \mid V^{(i)}Z = 0 \text{ and } R_i Z \neq 0\} \text{ and } \mathcal{Z}_1^{(i)} = \{Z \in \mathbb{F}_q^{n \times 1} \mid V^{(i)}Z = 0 \text{ and } R_i Z \neq 0\}.
$$

If L represents a linear $(\mathcal{I}, \delta)$-ECIC, then for all $Z \in \mathcal{Z}_t^{(i)}$ $w(LV^{(S)}Z) \geq 2\delta + 1$, where w counts the number of non-zero rows. On the other hand, if L realizes a linear $(\mathcal{I}', \delta)$-ECIC, then for all $Z \in \mathcal{Z}_1^{(i)}$, $w(LV^{(S)}Z) \geq 2\delta + 1$, where in this case the number of non-zero rows is the same of the non-zero entries of the $N \times 1$ vector $LV^{(S)}Z$. Note that any $Z \in \mathcal{Z}_t^{(i)}$ satisfies

$$
Z = [Z^1, ..., Z^t],
$$

with $Z^j \in \mathcal{Z}_1^{(i)} \cup \{0\}$ for all $j \in [t]$, and at least one is different from zero. Without loss of generality, suppose $Z_1 \neq 0$. Then if L represents a linear $(\mathcal{I}', \delta)$-ECIC we have

$$
LV^{(S)}Z = [LV^{(S)}Z^1, ..., LV^{(S)}Z^t]
$$

where the column $LV^{(S)}Z^1$ has at least $2\delta + 1$ non-zero entries, which implies that at least $2\delta + 1$ rows of $LV^{(S)}Z$ are non-zero.

Conversely, let $L \in \mathbb{F}_q^{N \times d_S}$ represent a linear $(\mathcal{I}, \delta)$-ECIC, and let $Z \in \mathcal{Z}_t^{(i)}$ such that

$$
Z = [\ Z^1, 0, ..., 0\ ],
$$

with $Z^1 \in \mathcal{Z}_1^{(i)}$. Then

$$
LV^{(S)}Z = [LV^{(S)}Z^1, 0, ..., 0]
$$

has at least $2\delta + 1$ non-zero rows, which means that $2\delta + 1$ entries of the first column are non-zero. Therefore L represents a linear $(\mathcal{I}', \delta)$-ECIC. ∎

For the remainder of this section, we fix $t = 1$, knowing that all the results hold also for $t > 1$ from Lemma IV.4.

We define the set:

$$
\mathcal{J}(\mathcal{I}) := \{U < \mathbb{F}_q^n : U \backslash \{0\} \subset \cup_{i \in [m]} \mathcal{Z}^{(i)}\}.
$$

We denote by $\alpha(\mathcal{I})$ the maximum dimension of any element of $\mathcal{J}(\mathcal{I})$, that is, the maximum dimension of any subspace of $\mathbb{F}_q^n$ in $\cup_{i \in [m]} \mathcal{Z}^{(i)} \cup \{0\}$.

We first give an extended α-bound, which gives a lower bound on the length of an optimal Hamming metric $(\mathcal{I}, \delta)$-ECIC. It may be helpful for the reader to think of this as the algebraic analogue of the independence number of a side-information graph.

Proposition IV.5. *(α-bound) Let $\mathcal{I}$ be an instance of the ICCSI problem. Then*

$$N(\alpha(\mathcal{I}), 2\delta + 1) \leq \mathcal{N}(\mathcal{I}, \delta).$$

Proof: Let $L \in \mathbb{F}_q^{N \times d_S}$ represent a linear $(\mathcal{I}, \delta)$-ECIC. Let $U \in \mathcal{J}(\mathcal{I})$ have dimension k and let G be a rank k matrix in $\mathbb{F}_q^{n \times k}$ such that $U = \{GX : X \in \mathbb{F}_q^k\}$. Let

$$C_U = \{LV^{(S)}GX : X \in \mathbb{F}_q^k\} \subset \mathbb{F}_q^N.$$

Then every element of $U \backslash \{0\}$ is contained in $\mathcal{Z}^{(i)}$ for some $i \in [m]$, so $w(LV^{(S)}GX) \geq 2\delta + 1$ for all non-zero $X \in \mathbb{F}_q^k$, by assumption. This furthermore implies that $LV^{(S)}G$ has rank k over $\mathbb{F}_q$. It follows that C_U is an $\mathbb{F}_q$-$[N, k, 2\delta + 1]$ code with $N \geq N(k, 2\delta + 1)$. Choosing U of maximal dimension in $\mathcal{J}(\mathcal{I})$ for an $(\mathcal{I}, \delta) - ECIC$ of optimal length we see that

$$N(\alpha(\mathcal{I}), 2\delta + 1) \leq \mathcal{N}(\mathcal{I}, \delta).$$

∎

We give sufficient conditions for tightness of the α-bound.

Corollary IV.6. *Let $\mathcal{I}$ be an instance of the ICCSI problem. If there exists a matrix $B \in \mathbb{F}_q^{\alpha(\mathcal{I}) \times d_S}$ satisfying $BV^{(S)^\perp} \cap V^{(i)^\perp} \subset R_i^\perp$ for all $i \in [m]$ then*

$$N(\alpha(\mathcal{I}), 2\delta + 1) = \mathcal{N}(\mathcal{I}, \delta).$$

Proof: Let $B \in \mathbb{F}_q^{\alpha(\mathcal{I}) \times d_S}$ satisfy the hypothesis of the corollary. Let G be a generator matrix for the $\mathbb{F}_q$-linear $[N, \alpha(\mathcal{I}), 2\delta + 1]$ code $\{GX : X \in \mathbb{F}_q^{d_S}\}$, and let $L = GB$. Then

$$w(LV^{(S)}Z) = w(GBV^{(S)}Z) \geq 2\delta + 1$$

whenever $BV^{(S)}Z \neq 0$. If $BV^{(S)}Z = 0$, then $Z \notin \mathcal{Z}^{(i)}$ for any $i \in [m]$ by our choice of B, so it follows that L represents an $\mathbb{F}_q$-linear Hamming metric $(\mathcal{I}, \delta)$-ECIC of length

$$N = N(\alpha(\mathcal{I}), 2\delta + 1) \geq \mathcal{N}(\mathcal{I}, \delta).$$

∎

Setting $\delta = 0$ in the above gives the following lower bound on the min-rank of an instance as an immediate consequence.

Corollary IV.7. *Let $\mathcal{I}$ be an instance of the ICCSI problem. Then*

$$\alpha(\mathcal{I}) \leq \kappa(\mathcal{I}),$$

with equality occurring if there exists $L \in \mathbb{F}_q^{\alpha(\mathcal{I}) \times d_S}$ satisfying $LV^{(S)^\perp} \cap V^{(i)^\perp} \subset R_i^\perp$ for all $i \in [m]$.

The reader will observe that in fact the condition $LV^{(S)^\perp} \cap V^{(i)^\perp} \subset R_i^\perp$ for each $i \in [m]$ is simply the equivalent statement to that of Lemma III.5, found by dualization.

Both the κ-bound and the Singleton bound hold in the context of coded-side information. The proofs are trivial extensions of those given in [11] and are retained here only for the convenience of the reader.

Proposition IV.8. *(κ-bound) Let $\mathcal{I}$ be an instance of the ICCSI problem. Then*

$$\mathcal{N}(\mathcal{I}, \delta) \leq N(\kappa(\mathcal{I}), 2\delta + 1).$$

Proof: Let $L_1 \in \mathbb{F}_q^{N_1 \times d_S}$ represent an optimal $\mathbb{F}_q$-linear $\mathcal{I}$-IC of length $N_1 = \kappa(\mathcal{I})$. Let $L_2 \in \mathbb{F}_q^{N \times N_1}$ have rank N_1, such that the code

$$C = \{L_2 X : X \in \mathbb{F}_q^{N_1}\} < \mathbb{F}_q^N$$

is an $[N, N_1, 2\delta + 1]$ linear code over $\mathbb{F}_q$ with $N = N(N_1, 2\delta + 1)$ for some δ. Since $LV^{(S)}Z \in \mathbb{F}_q^{N_1}$ is non-zero for all $Z \in \mathcal{S}(\mathcal{I})$,

$$w(L_2 L_1 V^{(S)} Z) \geq 2\delta + 1,$$

for all such Z. Then $L = L_2 L_1$ represents a linear $(\mathcal{I}, \delta)$-ECIC of length

$$N = N(\kappa(\mathcal{I}), 2\delta + 1) \geq \mathcal{N}(\mathcal{I}, \delta).$$

■

Proposition IV.9. *(Singleton bound) Let $\mathcal{I}$ be an instance of the ICCSI problem. Then*

$$\kappa(\mathcal{I}) + 2\delta \leq \mathcal{N}(\mathcal{I}, \delta).$$

Proof: Let $L \in \mathbb{F}_q^{N \times d_S}$ represent an optimal linear $(\mathcal{I}, \delta)$-ECIC over $\mathbb{F}_q$, so that $N = \mathcal{N}(\mathcal{I}, \delta)$. Let L' the matrix obtained by deleting any 2δ rows of L. By Theorem IV.2, for each $i \in [m]$,

$$w\left(LV^{(S)}Z\right) \geq 2\delta + 1, \quad \text{for all } Z \in \mathcal{Z}^{(i)},$$

so that

$$w\left(L'V^{(S)}Z\right) \geq 1, \quad \text{for all } Z \in \mathcal{Z}^{(i)}.$$

So L' is a linear index code of length $N - 2\delta$ for the instance $\mathcal{I}$. Now L' has at least $\kappa(\mathcal{I})$ rows so that

$$\kappa(\mathcal{I}) \leq \mathcal{N}(\mathcal{I}, \delta) - 2\delta.$$

■

Example IV.10. Let $m = 6, n = 5, q = 2$ and let $\mathcal{X}^{(S)} = \mathbb{F}_q^5$. Suppose that $\mathcal{X}^{(i)}$ has dimension $d_i = 2$ for each $i \in \{1, ..., 6\}$. Let $\mathcal{I}$ be the instance defined by user side-information

$$V^{(1)} = \begin{bmatrix} 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}, V^{(2)} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix}, V^{(3)} = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix},$$

$$V^{(4)} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \end{bmatrix}, V^{(5)} = \begin{bmatrix} 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}, V^{(6)} = \begin{bmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix},$$

and requests

$$R_1 = [10000], R_2 = [10000], R_3 = [00101], R_4 = [10001], R_5 = [11000], R_6 = [00111].$$

It can be checked that $\kappa(\mathcal{I}) = 3$. Moreover, $\cup_{i \in [6]} \mathcal{Z}^{(i)}$ contains the non-zero elements in the span of $\{(10110), (10011), (01100)\}$. Then $\alpha(\mathcal{I}) = \kappa(\mathcal{I}) = 3$. It follows from the α-bound that $6 = N(3, 3) = N(\alpha(\mathcal{I}), 3) \leq \mathcal{N}(\mathcal{I}, 1)$. From the κ-bound we have $6 = N(3, 3) = N(\kappa(\mathcal{I}), 3) \geq \mathcal{N}(\mathcal{I}, 1)$.

Reed-Solomon codes and their q-analogues in the form of Gabidulin codes [20] are examples of MDS and *maximum rank distance* (MRD) codes respectively. They were first introduced in [13]. In fact any extended generalized Reed-Solomon code over $\mathbb{F}_q$ is an MDS code of length $q + 1$ [23, Theorem 5.3.4] so the existence of such codes is assured for such lengths. It is conjectured that any $\mathbb{F}_q$-$[N, k, d]$ MDS code satisfies $N \leq q + 1$ unless q is even and $k = 3$ or $k = q - 1$ (in which case $N \leq q + 2$) [23].

Corollary IV.11. *Let $\mathcal{I}$ be an instance of the ICCSI problem. If $q \geq \kappa(\mathcal{I}) + 2\delta - 1$ then*

$$\mathcal{N}(\mathcal{I}, \delta) = \kappa(\mathcal{I}) + 2\delta.$$

Proof: If $q \geq \kappa(\mathcal{I}) + 2\delta - 1$ then there exists an $\mathbb{F}_q$-linear $[q + 1, \kappa(\mathcal{I}), 2\delta + 1]$ MDS code, namely an extended Reed-Solomon code. Then we obtain

$$\kappa(\mathcal{I}) + 2\delta \leq \mathcal{N}(\mathcal{I}, \delta) \leq N(k(\mathcal{I}), 2\delta + 1) = \kappa(\mathcal{I}) + 2\delta.$$

■

As usual, we let $V_q(n, r)$ be the size of a Hamming sphere of radius r in $\mathbb{F}_q^n$. We have the following generalization of [11, Theorem 6.1].

Theorem IV.12. *Let $\mathcal{I}$ be an instance of the ICCSI problem. Let $L \in \mathbb{F}_q^{N \times d_S}$ be selected uniformly at random over $\mathbb{F}_q$. The probability that L corresponds to a Hamming metric $\mathbb{F}_q$-linear $(\mathcal{I}, \delta)$-ECIC is at least*

$$1 - \sum_{i=1}^{m} q^{n - d_i - 1}(q - 1)\frac{V_q(N, 2\delta)}{q^N}.$$

In particular there exists an $\mathbb{F}_q$-linear $(\mathcal{I}, \delta)$-ECIC of length N if

$$N > n - d - 1 + \log_q(m(q - 1)V_q(N, 2\delta)),$$

where $d = \min\{d_i : i \in [m]\}$.

Proof: Let L be selected uniformly at random in $\mathbb{F}_q^{N \times d_S}$. If $w(LV^{(S)}Z) \leq 2\delta$ for some Z in $\mathcal{Z}^{(i)}$ then L is not δ-delta error correcting at the ith decoder. The probability of this occurring at the ith receiver is upper bounded by

$$\frac{|\mathcal{Z}^{(i)}|V_q(N, 2\delta)}{q^N} = q^{n-d_i-1-N}(q-1)V_q(N, 2\delta)$$

so from the union bound the probability of this occurring at some ith decoder is at most

$$\sum_{i \in [m]} q^{n-d_i-1-N}(q-1)V_q(N, 2\delta) \leq mq^{n-d-1}(q-1)\frac{V_q(N, 2\delta)}{q^N}.$$

∎

Remark IV.13. *If we let m'' denote the number of equivalence classes of $[m]$ under the relation $\hat{m}$ that i and j are equivalent if $\mathcal{Z}^{(i)} = \mathcal{Z}^{(j)}$, then in the above we obtain the following refinement: There exists an $\mathbb{F}_q$-linear $(\mathcal{I}, \delta)$-ECIC of length N if*

$$N > n - d - 1 + \log_q(m''(q-1)V_q(N, 2\delta)),$$

where $d = \min\{d_i : i \in [m]\}$.

Let H_q denote the q-ary entropy function:

$$H_q : (0,1) \to \mathbb{R} : x \mapsto x \log_q(q-1) - x \log_q(x) - (1-x) \log_q(1-x).$$

It is well known that the function $H_q(x)$ is continuous and increasing on $(0, 1 - (1/q))$. A proof of the following can be found in [28].

Lemma IV.14. *Let $\lambda \in (0, 1 - (1/q))$ be such that $n\lambda$ is an integer. Then*

$$V_q(n, \lambda n) \leq q^{H_q(\lambda)n}.$$

Corollary IV.15. *Let $\mathcal{I}$ be an instance of the ICCSI problem with. Let $\lambda \in \mathbb{Q}$ such that $0 < \lambda < 1 - 1/q$ and let $N \in \mathbb{Z}$ satisfy $\lambda N \in \mathbb{Z}$ Then, choosing the entries of $L \in \mathbb{F}_q^{N \times d_S}$ uniformly at random over the field $\mathbb{F}_q$, the probability that L corresponds to a Hamming metric $\mathbb{F}_q$-linear $(\mathcal{I}, \delta)$-ECIC, with $\delta = \lfloor \frac{\lambda N}{2} \rfloor$, is at least*

$$1 - (q-1) \sum_{i \in \hat{m}} \frac{q^{(n-d_i-1)}}{q^{N(1-H_q(\lambda))}}.$$

In particular there exists an $\mathbb{F}_q$-linear Hamming metric $(\mathcal{I}, \delta)$-ECIC if

$$m'' < \frac{q^{N(1-H_q(\lambda))-(n-d-1)}}{q-1},$$

where $d = \min\{d_i : i \in [m]\}$.

2) Rank Metric $(\mathcal{I}, \delta)$-ECICs: We assume throughout this section that $t > 1$, that w represents the rank weight and that $\mathcal{N}(\mathcal{I}, \delta)$ is the optimal length of an $\mathbb{F}_q$-linear rank metric $(\mathcal{I}, \delta)$-ECIC. Again, we fix some further notation. We let $N(t, \log_q M, d)$ denote the least integer s such that there exists a code in $\mathbb{F}_q^{s \times t}$ of minimum rank distance d and size M. We say that an $\mathbb{F}_q$-linear code of dimension k and minimum rank distance d in $\mathbb{F}_q^{n \times t}$ is a rank metric $\mathbb{F}_q$-$[n, k, d]$ code. In analogy with the previous section, we define the set:

$$\mathcal{J}(\mathcal{I}) := \{U \subset \mathbb{F}_q^{n \times t} : X - X' \in \cup_{i \in [m]} \mathcal{Z}_\delta^{(i)}, \text{for any } X, X' \in U\}.$$

and let $\alpha(\mathcal{I}) := \max\{\log_q |U| : U \in \mathcal{J}(\mathcal{I})\}$.

Theorem IV.16. *Let $\mathcal{I}$ be an instance of the ICCSI problem. Then*

$$N(t, \alpha(\mathcal{I}), 2\delta + 1) \leq \mathcal{N}(\mathcal{I}, \delta).$$

Proof: Let $L \in \mathbb{F}_q^{N \times t}$ represent an optimal $(\mathcal{I}, \delta)$-ECIC. Let $U \in \mathcal{J}(\mathcal{I})$ and define

$$C_U = \{LV^{(S)}X : X \in U\} \subset \mathbb{F}_q^{N \times t}.$$

Then C_U has minimum rank distance $2\delta + 1$ in $\mathbb{F}_q^{N \times t}$ since $w(LV^{(S)}(X - X')) \geq 2\delta + 1$ for any pair $X, X' \in U$. The result follows on choosing $U \in \mathcal{J}(\mathcal{I})$ such that $\log_q |U| = \alpha(\mathcal{I})$. ∎

The rank-distance Singleton bound [13] states that for any code C in $\mathbb{F}_q^{N \times t}$ of minimum distance $2\delta + 1$ that

$$\log_q |C| \leq \begin{cases} t(N - 2\delta) & \text{if } t \geq N \\ N(t - 2\delta) & \text{if } t \leq N \end{cases}$$

Codes that meet this bound are called maximum rank distance (MRD) codes. Combining the α-bound and the Singleton bound for rank-metric codes immediately yields the following.

Corollary IV.17. *(Singleton bound) Let $\mathcal{I}$ be an instance of the ICCSI problem. Then*

$$\mathcal{N}(\mathcal{I},\delta) \geq \begin{cases} \dfrac{\alpha(\mathcal{I})}{t} + 2\delta & \text{if } t \geq N(t,\alpha(\mathcal{I}),2\delta+1), \\ \dfrac{\alpha(\mathcal{I})}{t-2\delta} & \text{if } t \leq N(t,\alpha(\mathcal{I}),2\delta+1). \end{cases}$$

We now give a result on the existence of a linear encoding of length N for $(\mathcal{I},\delta)$-ECIC, extending Theorem 6.1 in [11]. We let $V_q(N,t,s) := |\{X \in \mathbb{F}_q^{N\times t} : w(X) \leq s\}|$ denote the size of a sphere of rank distance radius s in $\mathbb{F}_q^{N\times t}$.

We will use the following result from [27].

Theorem IV.18. *Let W be an $\mathbb{F}_q$-vector space and let $\mathcal{F}_r$ be a family of r-dimensional subspaces of W. Let $\mathrm{Hom}_{\mathcal{F}_r}(\mathbb{F}_q^t, W)$ denote the set of homomorphisms of $\mathbb{F}_q^t$ whose images lie in $\mathcal{F}_r$. Then*

$$|\mathrm{Hom}_{\mathcal{F}_r}(\mathbb{F}_q^t, W)| = |\mathcal{F}_r| \prod_{j=0}^{r-1}(q^t - q^j).$$

If W is a subspace of $\mathbb{F}_q^s$ then $\mathrm{Hom}_{\mathcal{F}_r}(\mathbb{F}_q^t, W)$ corresponds to the set of all $s \times t$ matrices of rank r whose column spaces lie in W.

Let m''' denote the number of equivalence classes of $[m]$ under the relation $\breve{m}$ that i and j are equivalent if $\mathcal{Z}_\delta^{(i)} = \mathcal{Z}_\delta^{(j)}$

Theorem IV.19. *Let $\mathcal{I}$ be of an instance of an ICCSI problem and let $L \in \mathbb{F}_q^{N\times d_S}$ for some positive integer N. The probability that L represents a linear $(\mathcal{I},\delta)$-ECIC of length N is at least*

$$1 - q^{-Nt} \sum_{i\in\breve{m}} \sum_{r\geq 2\delta+1} \left(\prod_{j=0}^{r-1}(q^{n-d_i} - q^j) - \prod_{j=0}^{r-1}(q^{n-d_i-1} - q^j)\right) \begin{bmatrix} t \\ r \end{bmatrix}_q \sum_{r=0}^{2\delta}\prod_{j=0}^{r-1}(q^N - q^j) \begin{bmatrix} t \\ r \end{bmatrix}_q.$$

In particular, there exists such a matrix L if

$$\sum_{i\in\breve{m}} \sum_{r\geq 2\delta+1} \left(\prod_{j=0}^{r-1}(q^{n-d_i} - q^j) - \prod_{j=0}^{r-1}(q^{n-d_i-1} - q^j)\right) \begin{bmatrix} t \\ r \end{bmatrix}_q < \frac{q^{Nt}}{V(N,t,2\delta)}.$$

Proof: From Theorem IV.2, the matrix $L \in \mathbb{F}_q^{N\times d_S}$ represents a linear $(\mathcal{I},\delta)$ if and only if for each $i \in [m]$, $w(LV^{(S)}Z) \geq 2\delta+1$ for any $Z \in \mathcal{Z}_\delta^{(i)}$. Therefore, a decoding failure at the ith node occurs if and only if the sphere $B_{2\delta}(Z) = \{LV^{(S)}Z+W : w(W) \leq 2\delta\} \subset \mathbb{F}_q^{N\times t}$ contains the zero matrix for some $Z \in \mathcal{Z}_\delta^{(i)}$. Then the probability of a decoding failure at the ith receiver is upper bounded by

$$\frac{\left|\cup_{Z\in\mathcal{Z}_\delta^{(i)}} B_{2\delta}(Z)\right|}{|\mathbb{F}_q^{N\times t}|} \leq \frac{|\mathcal{Z}_\delta^{(i)}|V(N,t,2\delta)}{q^{Nt}}.$$

We define the following sets for each non-negative integer r:

$$S_r^{(i)} = \{M < V^{(i)\perp} : \dim M = r\} \text{ and } T_r^{(i)} = \{M < V^{(i)\perp} \cap R_i^\perp : \dim M = r\}.$$

Then $|S_r^{(i)}| = \begin{bmatrix} n-d_i \\ r \end{bmatrix}_q$ and $|T_r^{(i)}| = \begin{bmatrix} n-d_i-1 \\ r \end{bmatrix}_q$. Now $S_r^{(i)}$ (resp. $T_r^{(i)}$) is the set of column spaces in $\mathbb{F}_q^n$ of all $n \times t$ matrices in $\mathcal{Y}^{(i)}$ (resp. in $\mathcal{W}^{(i)}$) of rank r. Then from Theorem IV.18, it follows that

$$\begin{aligned} |\mathcal{Z}_\delta^{(i)}| &= \sum_{r\geq 2\delta+1} \left(|\mathrm{Hom}_{S_r^{(i)}}(\mathbb{F}_q^t, V^{(i)\perp})| - |\mathrm{Hom}_{T_r^{(i)}}(\mathbb{F}_q^t, V^{(i)\perp} \cap R_i^\perp)|\right) \\ &= \sum_{r\geq 2\delta+1} \left(|S_r^{(i)}| - |T_r^{(i)}|\right) \prod_{j=0}^{r-1}(q^t - q^j) \\ &= \sum_{r\geq 2\delta+1} \left(\prod_{j=0}^{r-1}(q^{n-d_i} - q^j) - \prod_{j=0}^{r-1}(q^{n-d_i-1} - q^j)\right) \begin{bmatrix} t \\ r \end{bmatrix}_q. \end{aligned}$$

Theorem IV.18 can also be applied to obtain

$$V(N,t,2\delta) = \sum_{r=0}^{2\delta} |\mathrm{Hom}_r(\mathbb{F}_q^t, \mathbb{F}_q^N)| = \sum_{r=0}^{2\delta}\prod_{j=0}^{r-1}(q^N - q^j) \begin{bmatrix} t \\ r \end{bmatrix}_q.$$

$t \geq$	$d \geq$	$N \geq$	$\delta \leq$	$m \leq$
6	11	16	1	239
7	11	15	1	239
8	12	13	1	239
11	12	12	1	239
20	12	11	1	239
10	11	20	2	239
11	11	19	2	239
12	11	18	2	239
14	11	17	2	239
17	11	16	2	239
9	12	19	2	239
10	12	18	2	239
11	12	17	2	239
13	12	16	2	239
16	12	15	2	239
16	12	19	3	239
19	12	18	3	239
13	13	20	3	239
14	13	19	3	239
15	13	18	3	239
16	13	18	3	239
17	13	17	3	239
18	13	18	3	239
19	13	17	3	239

TABLE IV

Then the probability of a failure at the ith decoder is upper-bounded by

$$q^{-Nt} \sum_{r \geq 2\delta+1} \left(\prod_{j=0}^{r-1}(q^{n-d_i} - q^j) - \prod_{j=0}^{r-1}(q^{n-d_i-1} - q^j) \right) \begin{bmatrix} t \\ r \end{bmatrix}_q \sum_{r=0}^{2\delta} \prod_{j=0}^{r-1}(q^N - q^j) \begin{bmatrix} t \\ r \end{bmatrix}_q .$$

The result now follows from the union bound. ∎

In the error-free case, that is for $\delta = 0$, Theorem IV.19 asserts that there exists an $N \times d_S$ matrix L of rank N representing an $\mathbb{F}_q$-linear $\mathcal{I}$-IC whenever

$$1 > \sum_{i \in \check{m}} \frac{|\mathcal{Z}^{(i)}|}{q^{Nt}} = \sum_{i \in \check{m}} q^{(n-d_i-N-1)t}(q^t - 1).$$

Moreover

$$m''' q^{(k-N-1)t}(q^t - 1) \geq \sum_{i \in \check{m}}^{m} q^{(n-d_i-N-1)t}(q^t - 1)$$

where $k = \max\{n - d_i : i \in [m]\}$. Then for $N = k + \ell$, there exists a linear $\mathcal{I}$ of length N as long as $m''' \leq q^{(\ell+1)t}/(q^t - 1)$. In particular, this shows that:

Corollary IV.20. *Let $\mathcal{I}$ be an instance of the of the ICCSI problem and let $k = \max\{n - d_i : i \in [m]\}$. If $m''' \leq q^{\ell t}/(q^t - 1)$ then $\kappa(\mathcal{I}) \leq k + \ell - 1$.*

In Table IV we give parameters t, N, δ for which the existence if a linear $(\mathcal{I}, \delta)$-ECIC of length N is established by Theorem IV.19 for $n = 20$, $d_i = d$ for each $i \in [m]$.

V. DECODING INDEX CODES

Error correction for index codes (as for non-multicast network codes) is non-trivial. We consider two approaches, one for rank-metric error correction and the other to correct Hamming metric errors, based on syndrome decoding.

A. Syndrome Decoding for Hamming Metric Errors

In [11] the authors give a syndrome decoding algorithm for Hamming metric error correction in the ICSI problem. In this section we extend the algorithm to the case of ICCSI problem.

For the remainder of this section, we let $L \in \mathbb{F}_q^{N \times d_S}$ be a matrix corresponding to an $(\mathcal{I}, \delta)$-ECIC. Suppose that for some $i \in [m]$ the ith user, receives the message

$$Y_{(i)} = LV^{(S)}X + W_{(i)} \in \mathbb{F}_q^{N \times t},$$

where $LV^{(S)}X$ is the codeword transmitted by S and $W_{(i)}$ is the error vector in $\mathbb{F}_q^N$. Since $R_i \notin \mathcal{X}^{(i)}$, there exists an invertible matrix $M_{(i)} \in \mathbb{F}_q^{n \times n}$ such that

$$V^{(i)}M_{(i)} = [I|0] \text{ where } I \text{ is the identity matrix in } \mathbb{F}^{d_i \times d_i}, \text{ and } R_i M_{(i)} = \mathbf{e}_{d_i+1}.$$

The matrix $M_{(i)}$ may be constructed by the ith user as follows. Choose a right inverse $A_{(i)} \in \mathbb{F}_q^{n \times d_i+1}$ of the matrix $G \in \mathbb{F}_q^{d_i+1 \times n}$ that has the rows of $V^{(i)}$ as its first d_i rows and has R_i in the final row. Then $GA_{(i)}$ is the identity matrix in $\mathbb{F}_q^{(d_i+1) \times (d_i+1)}$ so that

$$V^{(i)}A_{(i)}^{d_i+1} = 0, V^{(i)}A_{(i)}^{[d_i]} = I, R_i A_{(i)} = [0, ..., 0, 1].$$

Choose $B_{(i)}$ to be an $n \times (n - d_i - 1)$ matrix whose columns form a basis of $G^{\perp}$. Then $M_{(i)} = [A_{(i)}|B_{(i)}]$ is invertible and satisfies $V^{(i)}M_{(i)} = [I|0]$ and $R_i M_{(i)} = \mathbf{e}_{d_i+1}$.

Now define $X' := M_{(i)}^{-1}X \in \mathbb{F}_q^{n \times t}$. Then we have

$$V_j^{(i)}X = \mathbf{e}_j M_{(i)}^{-1}X = X_j' \text{ for } j \in [d_i]$$

and

$$R_i X = \mathbf{e}_{d_i+1} M_{(i)}^{-1} X = X_{d_i+1}'.$$

Lemma V.1. *If $Z \in [I|0]^{\perp}$ and $Z_{d_i+1} \neq 0$ then*

$$w(LV^{(S)}M_{(i)}Z) \geq 2\delta + 1.$$

Proof: Let $Z \in [I|0]^{\perp}$ be such that $Z_{d_i+1} \neq 0$. Then $V^{(i)}M_{(i)}Z = [I|0]Z = 0$ and $R_i M_{(i)}Z = \mathbf{e}_{d_i+1}Z = Z_{d_i+1} \neq 0$ so $M_{(i)}Z \in \mathcal{Z}^{(i)}$. The result now follows from Theorem IV.2. ∎

Let $L' = LV^{(S)}M_{(i)}$ and let $\overline{[s]} := [n] \setminus [s]$. Consider the following two codes. We define $\mathcal{C}^{(i)} \subset \mathbb{F}_q^N$ to be the column space of the matrix $[L'^{d_i+1}|L'^{\overline{[d_i+1]}}] \in \mathbb{F}_q^{N \times n}$ and we define $\mathcal{C}_{(i)} \subset \mathbb{F}_q^N$ to be the subspace of $\mathcal{C}^{(i)}$ spanned by the columns of $L'^{\overline{[d_i+1]}}$.

For each $i \in [m]$, we have $\mathcal{C}_{(i)} \subseteq \mathcal{C}^{(i)}$ with $\dim(\mathcal{C}^{(i)}) = \dim(\mathcal{C}_{(i)}) + 1$. As usual, for an $\mathbb{F}_q$-linear code $C \in \mathbb{F}_q^N$ we write $C^{\perp} := \{y \in \mathbb{F}_q^N : x \cdot y = 0\}$ to denote its dual code. Then we have $\mathcal{C}^{(i)\perp} \subseteq \mathcal{C}_{(i)}^{\perp}$ with $r_i = \dim(\mathcal{C}_{(i)}^{\perp}) = \dim(\mathcal{C}^{(i)\perp}) + 1$ for some r_i. Let $H_{(i)}$ be a parity check matrix of $\mathcal{C}_{(i)}$ of the form

$$H_{(i)} = \left[\frac{h_{(i)}}{H^{(i)}}\right] \in \mathbb{F}_q^{r_i \times N}, \tag{3}$$

where $H^{(i)}$ is a parity check matrix of $\mathcal{C}^{(i)}$ and $h_{(i)} \in \mathcal{C}_{(i)}^{\perp} \setminus \mathcal{C}^{(i)\perp}$.

Then

$$H_{(i)}L'^{d_i+1} = [s_{d_i+1}, 0, \ldots, 0]^T$$

for some $s_{d_i+1} \in \mathbb{F}_q \setminus \{0\}$.

We now outline a procedure for decoding the demand $R_i X$ at the ith receiver, which is based on syndrome decoding. In the first step we compute syndrome, of $H_{(i)}$, in which is embedded a syndrome of $H^{(i)}$. In the second step a table of syndromes is computed for the code $\mathcal{C}^{(i)}$. Finally, in the third step the output $R_i X$ is computed.

Step I: Compute

$$H_{(i)}(Y_{(i)} - L'^{[d_i]}X_{[d_i]}') = \begin{bmatrix} \alpha_i \\ \beta_i \end{bmatrix} \in \mathbb{F}_q^{r_i \times t} \tag{4}$$

Step II: Find $\varepsilon \in \mathbb{F}_q^{N \times t}$ with $w(\varepsilon) \leq \delta$ such that

$$H^{(i)}\varepsilon = \beta_i \in \mathbb{F}_q^{(r_i-1) \times t}. \tag{5}$$

Step III: Compute

$$\hat{X}_{d_i+1} = (\alpha_i - h_{(i)}\varepsilon)/s_{d_i+1}. \tag{6}$$

Theorem V.2. *If $w(W_{(i)}) \leq \delta$ then the procedure above has output $\hat{X}_{d_i+1} = X_{d_i+1}' = R_i X$.*

Proof: We have

$$
\begin{aligned}
Y_{(i)} &= LV^{(S)}X + W_{(i)} \\
&= LV^{(S)}M_{(i)}M_{(i)}^{-1}X + W_{(i)} \\
&= L'X' + W_{(i)} \\
&= L'^{[d_i]}X'_{[d_i]} + L'^{\overline{[d_i+1]}}X'_{\overline{[d_i+1]}} + L'^{d_i+1}X'_{d_i+1} + W_{(i)},
\end{aligned}
$$

and

$$
Y_{(i)} - L'^{[d_i]}X'_{[d_i]} = L'^{\overline{[d_i+1]}}X'_{\overline{[d_i+1]}} + L'^{d_i+1}X'_{d_i+1} + W_{(i)}.
$$

Then

$$
H_{(i)}(Y_{(i)} - L'^{[d_i]}X'_{[d_i]}) = \left[\begin{array}{c} \alpha_i \\ \beta_i \end{array} \right]
$$

where $\alpha_i = s_{d_i+1}X_{d_i+1} + h_{(i)}W_{(i)} \in \mathbb{F}_q^{1\times t}$ and $\beta_i = H^{(i)}W_{(i)} \in \mathbb{F}_q^{(r_i-1)\times t}$.

Let $\varepsilon \in \mathbb{F}_q^{N\times t}$ have Hamming weight at most δ, as in Step II. Then $W_{(i)} - \varepsilon \in \mathcal{C}^{(i)}$ and $w(W_{(i)} - \varepsilon) \le 2\delta$, which means $W_{(i)} - \varepsilon \in \mathcal{C}_{(i)}$ from Lemma V.1. Therefore,

$$
(\alpha_i - h_{(i)}\varepsilon)/s_{d_i+1} = (s_{d_i+1}X'_{d_i+1} + h_{(i)}(W_{(i)} - \varepsilon))/s_{d_i+1} = X'_{d_i+1}.
$$

∎

Example V.3. Let $q = 2$, $m = n = 4$, $t = 1$, $\delta = 1$ and $R_i = \mathbf{e}_i$ for all $i \in [4]$ and $\mathcal{X}^{(S)} = \mathbb{F}_2^4$.

Assume

$$
V^{(1)} = \left[\begin{array}{cccc} 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{array} \right], V^{(2)} = \left[\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{array} \right],
$$

$$
V^{(3)} = \left[\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{array} \right], V^{(4)} = \left[\begin{array}{cccc} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{array} \right].
$$

Then

$$
\cup_{i\in[4]}\mathcal{Z}^{(i)} = \{[1001], [1000], [0111], [0100], [0010], [0110]\},
$$

so that $\alpha(\mathcal{I}) = 2$. In fact $\langle[0100], [0010]\rangle \setminus \{0\} \subset \cup_{i\in[4]}\mathcal{Z}^{(i)}$, and from the α-bound we have $5 = N(2,3) \le \mathcal{N}(\mathcal{I}, 1)$. It can be checked that $\kappa(\mathcal{I}) = 2$, and so from the κ-bound we have $5 = N(2,3) \ge \mathcal{N}(\mathcal{I}, 1)$. Then

$$
L = \left[\begin{array}{cccc} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{array} \right]
$$

represents an optimal linear $(\mathcal{I}, 1)$-ECIC.

Let $X = [1111]^T$. The sender broadcasts LX. Suppose one Hamming error occurs and U_4 receives the vector $Y_4 = LX + W_{(4)}$, where

$$
W_{(4)} = [00010].
$$

Then

$$
Y_4 = [01001].
$$

Let

$$
M_{(4)} = \left[\begin{array}{cccc} 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{array} \right] \quad \text{and} \quad L' = LM_{(4)} = \left[\begin{array}{cccc} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 \end{array} \right]
$$

We obtain a parity check matrix of $\mathcal{C}_{(4)}$, as in (3)

$$
H_{(4)} = \left[\begin{array}{ccccc} 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{array} \right].
$$

Applying Step I of our decoding algorithm we obtain

$$H_{(4)}(Y - L'^{[2]}X'_{[2]}) = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix}.$$

Therefore $\alpha_4 = 0$ and $\beta_4 = [111]^T$. Now from Step II, we obtain that the vector $\varepsilon = [00001]^T$ is a solution of (5) and in Step III we obtain

$$\hat{X}_3 = (0 - [00011] \cdot [00001])/1 = 1 = X_4.$$

Remark V.4. *The above outlined decoding procedure extends that of [11, Section VII] to the ICCSI case, firstly via the use of the matrices $M_{(i)}$, which transform it to an ICSI problem for the user i. However, Step III of our algorithm diverges from that one in a different sense: in [11] it is required to solve the system $Y_i = L\bar{X} - \varepsilon$ given $\bar{X}$ whose coordinates agree with those of X in the side-information of the ith user, for any decoding. In our case a pre-computation is performed to determine $h_{(i)}$ as in (3) and s_{d_i+1}. We do this by solving the system*

$$h_{(i)} \left[L'^{d_i+1} \;\middle|\; L'^{\overline{[d_i]}} \right] = [1, 0, ..., 0].$$

The computational complexities of both algorithms are similar, being dominated by Step II, where a low weight element of a coset of $\mathcal{C}^{(i)}$ must be found.

B. Decoding for Rank-Metric Errors

In the model presented here, we assume that a matrix Y is transmitted and that at any given receiver, a matrix of the form $Y + W$ is received. Therefore the decoding algorithm of the additive matrix channel as described in [35] may be considered. We do not in fact necessarily assume that L represents an $(\mathcal{I}, \delta)$-ECIC. Instead we add redundancy by embedding the broadcast $LV^{(S)}X$ into a larger matrix with zeroes off the entries assigned to $LV^{(S)}X$. In this scheme, it is assumed that up to r packets are randomly injected into the network, in the form of a matrix of rank r. It can be assumed that with high probability, the first r rows of the error matrix are linearly independent.

Given a $N \times d_S$ matrix L over $\mathbb{F}_q$ for an $\mathcal{I}$-IC each ith receiver requires $LV^{(S)}$ and $LV^{(S)}X$ in order to retrieve its requested data $R_i X$. Employing the method of [35], we let

$$P = \begin{pmatrix} 0_{v \times v} & 0_{v \times \ell} \\ 0_{N \times v} & Q \end{pmatrix},$$

where $Q = LV^{(S)}X \in \mathbb{F}_q^{N \times t}$ and $\ell = t$ if L is known to each receiver and $Q = [LV^{(S)}|LV^{(S)}X] \in \mathbb{F}_q^{N \times (d_S+t)}$ and $\ell = d_S + t$ if $LV^{(S)}$ is not known to all receivers.

Given an error matrix W of rank $r \leq v$, we write

$$W = \begin{pmatrix} W_{11} & W_{12} \\ W_{21} & W_{22} \end{pmatrix},$$

with $W_{11} \in \mathbb{F}_q^{v \times v}$, $W_{21} \in \mathbb{F}_q^{N \times v}$, $W_{12} \in \mathbb{F}_q^{v \times t}$, $W_{22} \in \mathbb{F}_q^{N \times t}$. If W_{11} has rank r then

$$r = \text{rank}(W_{11}) \leq \text{rank}\begin{pmatrix} W_{11} \\ W_{21} \end{pmatrix} \leq \text{rank}(W) = r,$$

so the rows of W_{21} are contained in the row space of W_{11}. Therefore, $TW_{11} = W_{21}$ for some $T \in \mathbb{F}_q^{N \times v}$. Then

$$r = \text{rank}(W) = \text{rank}(W_{11}) + \text{rank}(TW_{12} - W_{22}) = r + \text{rank}(TW_{12} - W_{22}),$$

so we must have $TW_{12} = W_{22}$. The matrix T can be easily computed, since the submatrices W_{11}, W_{21} are known to each receiver. Moreover, since W_{12} is known, the decoder retrieves $Q = -TW_{12} + W_{22} + Q$.

From Lemma III.5, the matrix L represents an $\mathbb{F}_q$-linear $\mathcal{I}$-IC if and only if for each $i \in [m]$ there exist vectors $U \in \mathbb{F}_q^n, A \in \mathbb{F}_q^{d_i}$ and $B \in \mathbb{F}_q^N$ such that

$$R_i = AV^{(i)} - BLV^{(S)} \text{ and } U = AV^{(i)}.$$

Once $LV^{(S)}$ and $LV^{(S)}X$ is known at the ith receiver, its requested data $R_i X$ can be computed as follows.

1) Choose $U \in \mathcal{X}^{(i)}$. Equivalently, choose $A \in \mathbb{F}_q^{d_i}$ and write $U = AV^{(i)}$.
2) Solve $R_i + AV^{(i)} = BLV^{(S)}$ for some $B \in \mathbb{F}_q^N$.
3) Compute $R_i X = BY - A\Lambda^{(i)}$.

In practice, the decoder computes $[S|T]$, the reduced-row echelon form of the matrix

$$\begin{bmatrix} V^{(i)} & \Lambda^{(i)} \\ LV^{(S)} & Y \end{bmatrix}$$

and solves for Z in $ZS = R_i$ to retrieve $R_i X = ZT$. In particular, if $R_i = \mathbf{e}_j$ for some $j \in [N]$, then R_i already appears as a row of P, and the corresponding row of Q gives the required vector sought.

Note that the method of [35] assumes that the error matrix W has its first r rows linearly independent. This assumption is referred to by the authors as *error-trapping*. In the event that $\text{rank}(W_{11}) < \text{rank}\begin{pmatrix} W_{11} \\ W_{21} \end{pmatrix}$, the decoder detects that error-trapping has failed to occur. If $\text{rank}(W_{11}) = \text{rank}\begin{pmatrix} W_{11} \\ W_{21} \end{pmatrix} < \text{rank}(W)$, the decoder does not detect that error-trapping has failed, so a decoding failure will occur. As noted in [35] this probability is less than $\frac{2r}{q^{1+v-r}}$.

Remark V.5. *For the case $t > 1$, if L does represent a rank-metric $(\mathcal{I}, \delta)$-ECIC, and $LV^{(S)}$ is known to each receiver in advance of the transmission, then the sender may broadcast*

$$P = \begin{bmatrix} 0_{v \times v} & 0_{v \times t} \\ 0_{N \times v} & LV^{(S)}X \end{bmatrix}$$

While the ith client receives the noisy transmission:

$$P + W = \begin{bmatrix} W_{11} & W_{12} \\ W_{21} & W_{22} + LV^{(S)}X \end{bmatrix}.$$

If error-trapping has failed and this is detected at the ith decoder then from Theorem IV.2, if $\text{rank}(W_{22}) \leq \delta$ then $R_i X$ is uniquely retrievable from the submatrix $[W_{22} + LV^{(S)}X]$. However, the existence of an efficient algorithm to compute $R_i X$ given the received matrix $[W_{22} + LV^{(S)}X]$ for an arbitrary matrix L representing an $(\mathcal{I}, \delta)$-ECIC is unlikely.

Example V.6. Let $m = 4, n = 4, q = 2$ and let $\mathcal{X}^{(S)} = \mathbb{F}_q^4$. Suppose that $\mathcal{X}^{(i)}$ has dimension $d_i = 1$ for each $i \in \{1, ..., 4\}$. Let $\mathcal{I}$ be the instance defined by user side-information

$$V^{(1)} = \begin{bmatrix} 0 & 1 & 0 & 0 \end{bmatrix}, V^{(2)} = \begin{bmatrix} 0 & 0 & 1 & 0 \end{bmatrix}, V^{(3)} = \begin{bmatrix} 0 & 0 & 0 & 1 \end{bmatrix}, V^{(4)} = \begin{bmatrix} 1 & 0 & 0 & 0 \end{bmatrix},$$

and requests

$$R_1 = [1000], R_2 = [0100], R_3 = [0010], R_4 = [0001].$$

It can be checked that $\kappa(\mathcal{I}) = 3$ and that

$$L = \begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$$

is a matrix corresponding to an $\mathcal{I}$-IC. Let $v = 2$, $t = 1$, $X = [1010]$ and suppose that L is known to the receivers. Then the matrix P is given by

$$P = \begin{pmatrix} 0_{2 \times 2} & 0_{2 \times 1} \\ 0_{3 \times 2} & LX \end{pmatrix}.$$

Now, suppose a user receives the matrix

$$P + W = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{bmatrix}; \text{ which implies } W = \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 0 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$$

Clearly, the error-trapping has succeeded, since the 2×2 upper left-hand submatrix of W has rank 2. Then we have

$$W_{11} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}, W_{21} = \begin{bmatrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \end{bmatrix},$$

from which we determine

$$T = \begin{bmatrix} 0 & 0 \\ 1 & 1 \\ 1 & 0 \end{bmatrix}.$$

From the bottom right-hand part of $P + W$ we compute

$$\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} - TW_{12} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} - \begin{bmatrix} 0 & 0 \\ 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = LX.$$

At this point the client can decode its demanded message.

VI. CONCLUSIONS

Permitting coded-side information in the index coding problem offers more potential for applications. While the connections to graphs and hypergraphs are no longer apparent as in the classical case, many of the associated combinatorial characterisations have algebraic interpretations. The ICCSI problem in some sense may be viewed as a q-analogue of the ICSI problem: the index set of size d_i of the side information of the ith user now being replaced by a vector space of dimension d_i. This viewpoint means that most bounds on the optimal length of an index code, both for noiseless and noisy channels have analogues in the more general setting of the ICCSI problem. Although it is likely that error-correcting decoding schemes for multicast network coding can be adapted for their index coding equivalents, the design of efficient error-correcting decoding algorithms for index codes remains a challenging problem.

VII. ACKNOWLEDGEMENT

REFERENCES

[1] N. Alon, A. Hassidim, E. Lubetzky, U. Stav, and A. Weinstein, "Broadcasting with Side Information", in Proc. 49th Annu. IEEE Symp. on Found. of Comput. Sci. (FOCS), pp. 823832, 2008.

[2] F. Arbabjolfaei and Y. H. Kim, "Structural Properties of Index Coding Capacity using Fractional Graph Theory", 2015 IEEE International Symposium on Information Theory (ISIT), June 2015, pp. 1034–1038.

[3] E. F. Assmus Jr., and J. D. Key, "Designs and Their Codes", Cambridge Univ. Press (1992).

[4] Z. Bar-Yossef, Z. Birk, T. S. Jayram, and T. Kol, "Index Coding with Side Information", in Proc. 47th Annu. IEEE Symp. Found. Comput. Sci., 2006, pp. 197–206.

[5] Z. Bar-Yossef, Z. Birk, T. S. Jayram, and T. Kol, "Index Coding with Side Information", IEEE Transactions on Information Theory, vol. 57, no. 3, pp. 1479–1494, Mar. 2011.

[6] Y. Birk and T. Kol, "Informed Source Coding on Demand (ISCOD) over Broadcast Channels", in Proc. IEEE Conf. Comput. Commun., San Francisco, CA, 1998, pp. 1257–1264.

[7] A. Blasiak, R. Kleinberg, E. Lubetsky, "Broadcasting With Side Information: Bounding and Approximating the Broadcast Rate," IEEE Transactions on Information Theory, vol. 59, no. 9, 2013, pp. 5811–5823.

[8] E. Byrne and M. Calderini, "Bounding the Optimal Rate of the ICSI and ICCSI Problems,", arXiv preprint 1604.05991, 2016.

[9] K. Chouinard, "Weight Distributions of Codes from Planes", PhD Thesis, University of Virginia, August 1998.

[10] MingJun Dai, K. W. Shum, Chi Wan Sung, "Data Dissemination With Side Information and Feedback," IEEE Transactions on Wireless Communications, Vol. 13, 9, pp. 4708–4720, 2014.

[11] Son Hoang Dau, V. Skachek, and Yeow Meng Chee, "Error Correction for Index Coding With Side Information", IEEE Transactions on Information Theory, Vol. 59 , Issue: 3, pp. 1517 - 1531, 2013.

[12] Son Hoang Dau, V. Skachek, and Yeow Meng Chee, "On the Security of Index Coding With Side Information", IEEE Transactions on Information Theory, vol.58, no.6, June 2012, pp. 3975–3988.

[13] P. Delsarte, "Bilinear Forms Over a Finite Field with Applications to Coding Theory," Journal of Combinatorial Theory Series A, 1978 25, 3, pp.226-241

[14] R. A. De Millo, R. J. Lipton, "A Probabilistic Remark on Algebraic Program Testing," Information Processing Letters 7 (4): pp. 193–195, 1978.

[15] M. Effros, S. El Rouayheb, M. Langberg, "An Equivalence Between Network Coding and Index Coding," IEEE Transactions on Information Theory, (61), No. 5, pp. 2478–2487, 2015.

[16] Maddah-Ali, Mohammad Ali, and Urs Niesen. "Fundamental limits of caching," IEEE Transactions on Information Theory 60.5 (2014): 2856-2867.

[17] Z. Chen, "Fundamental limits of caching: Improved bounds for small buffer users," arXiv preprint arXiv:1407.1935v1, Jul. 2014.

[18] Wan, Kai, Daniela Tuninetti, and Pablo Piantanida. "On the optimality of uncoded cache placement," arXiv preprint arXiv:1511.02256 Nov. 2015.

[19] C. Fragouli and E. Soljanin, "Network Coding Fundamentals," Foundations and Trends in Networking. Hanover, MA: (now Publishers Inc.), vol. 2, no. 1, 2007.

[20] E Gabidulin, "Theory of Codes with Maximum Rank Distance", Problems of Information Transmission, 21:1, pp.1–12, 1985.

[21] W. Haemers, "An Upper Bound for the Shannon Capacity of a Graph", Algebr. Methods Graph Theory, 25, 1978,pp. 267–272.

[22] Xiao Huang; S. El Rouayheb, "Index Coding and Network Coding via Rank Minimization," IEEE Information Theory Workshop (ITW), pp.14–18, 2015.

[23] W. C. Huffman and Vera Pless, "Fundamentals of Error-Correcting Codes", Cambridge University Press, 2003.

[24] M. Klemm, " Uber den p-Rang von Inzidenzmatrizen", J. Combin. Theory (A), 43, 1986, 138–139.

[25] Kötter, Kschischang, "Coding for Erasures and Errors in Random Network Coding," IEEE Transactions on Information Theory, (54), 8, 2008.

[26] R. Koetter, and M. Medard, "An Algebraic Approach to Network Coding", IEEE/ACM Trans. Netw., vol. 11, no. 5, pp. 782–795, Oct. 2003.

[27] D. Laksov, A. Thorup, "Counting Matrices with Coordinates in Finite Fields and of Fixed Rank," Math. Scand. 74, 1994, pp.19-33.

[28] H. Loeliger, "An Upper Bound on the Volume of Discrete Spheres", IEEE Transactions on Information Theory, (40), No. 6, pp. 2071–2073, 1994.

[29] H. Maleki, V. Cadambe, S. A. Jafar, "Index Coding - An Interference Alignment Perspective," IEEE Transactions on Information Theory, (60), No. 9, pp. 5402–5432, 2014.

[30] R. Peeters, "Orthogonal Representations over Finite Fields and the Chromatic Number of Graphs", Combinatorica, vol. 16, no. 3, pp. 417–431, 1996.

[31] A. E. Rouayheb, A. Sprintson, and C. Georghiades, "On the Index Coding Problem and its Relation to Network Coding and Matroid Theory", IEEE Transactions on Information Theory, vol. 56, no. 7, pp. 3187–3195, Jul. 2010.

[32] J. Schwartz, "Fast Probabilistic Algorithms for Verification of Polynomial Identities", Journal of the ACM 27: 701717, 1980.

[33] K. Shanmugan, A. Dimakis, M. Langberg, "Graph Theory versus Minimum-Rank for Index Coding", Proceedings of the 2014 IEEE International Symposium on Information Theory (ISIT) (full-paper at arXiv:1402.3898.v1, Feb 2014), pp. 291-295, 2014.

[34] K. W. Shum, Dai Mingjun, Chi Wan Sung, "Broadcasting with Coded Side Information", 2012 IEEE 23rd International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), vol. 89, no. 94, pp. 9–12, Sept. 2012.

[35] D. Silva, F. R. Kschischang, R. Koetter, "Communication Over Finite-Field Matrix Channels",IEEE Trans. Inf. Theory, vol. 56, no. 3, pp. 1296–1305, Mar. 2010.

[36] Silva, Kschischang, Kötter, "A Rank-Metric Approach to Error Control in Random Network Coding," IEEE Trans. Inform. Th. (54), 9, 2008.

[37] A. S. Tehrani, A. G. Dimakis, M. J. Neely, "Bipartite Index Coding," Proceedings of the IEEE 2012 International Symposium on Information Theory (ISIT), Boston, Jul 1-6, 2012, pp. 2246-2250.

[38] R. Zippel, "Probabilistic algorithms for sparse polynomials," Symbolic and Algebraic Computation, Lecture Notes in Computer Science, vol. 72, pp. 216–226, 1979.